**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION**

ST. LUKE TECHNOLOGIES, LLC ,	
Plaintiff,	Civil Action No._____
v.	
APPLE, INC.,	**JURY TRIAL DEMANDED**
Defendant.	

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff St. Luke Technologies, LLC ("St. Luke" or "Plaintiff"), by and through its attorneys, brings this action and makes the following allegations of patent infringement relating to U.S. Patent Nos. 8,316,237 ("the '237 patent"); 7,181,017 ("the '017 patent"); 7,869,591 ("the '591 patent"); 8,904,181 ("the '181 patent"); 7,587,368 ("the '368 patent"); 8,498,941 ("the '941 patent"; and 8,566,247 ("the '247 patent") (collectively, the "patents-in-suit"). Defendant Apple, Inc. ("Apple" or "Defendant") infringes the patents-in-suit in violation of the patent laws of the United States of America, 35 U.S.C. § 1 *et seq*.

INTRODUCTION

1.   In an effort to expand its product base and profit from the sale of infringing cloud computing encryption technologies and information record infrastructure technologies, Apple has unlawfully and without permission copied the technologies and inventions of Dr. Robert H. Nagel, David P. Felsher, and Steven M. Hoffberg.

2.   Dr. Nagel, Mr. Felsher, and Mr. Hoffberg are the co-inventors of the '237, '017, '591, '181, and '247 patents (collectively, the "Secure Third-Party Communications Patents" or "STPC patents"). The STPC patents have been cited in over 550 United States patents and patent applications as prior art before the United States Patent and Trademark Office. The STPC

patents disclose systems and methods for secure communications over a computer network

where a third party (intermediary) performs a requisite function with respect to the transaction

without requiring the intermediary to be trusted with respect to the private information or

cryptographic keys for communicated information. The inventions taught in the STPC patents

employ secure cryptographic schemes, which drastically reduce the risk of unauthorized

disclosure of encrypted data.

     3.   The below diagram shows St. Luke's STPC patents, pending STPC patent

applications, and the STPC patents Apple infringes.[1]
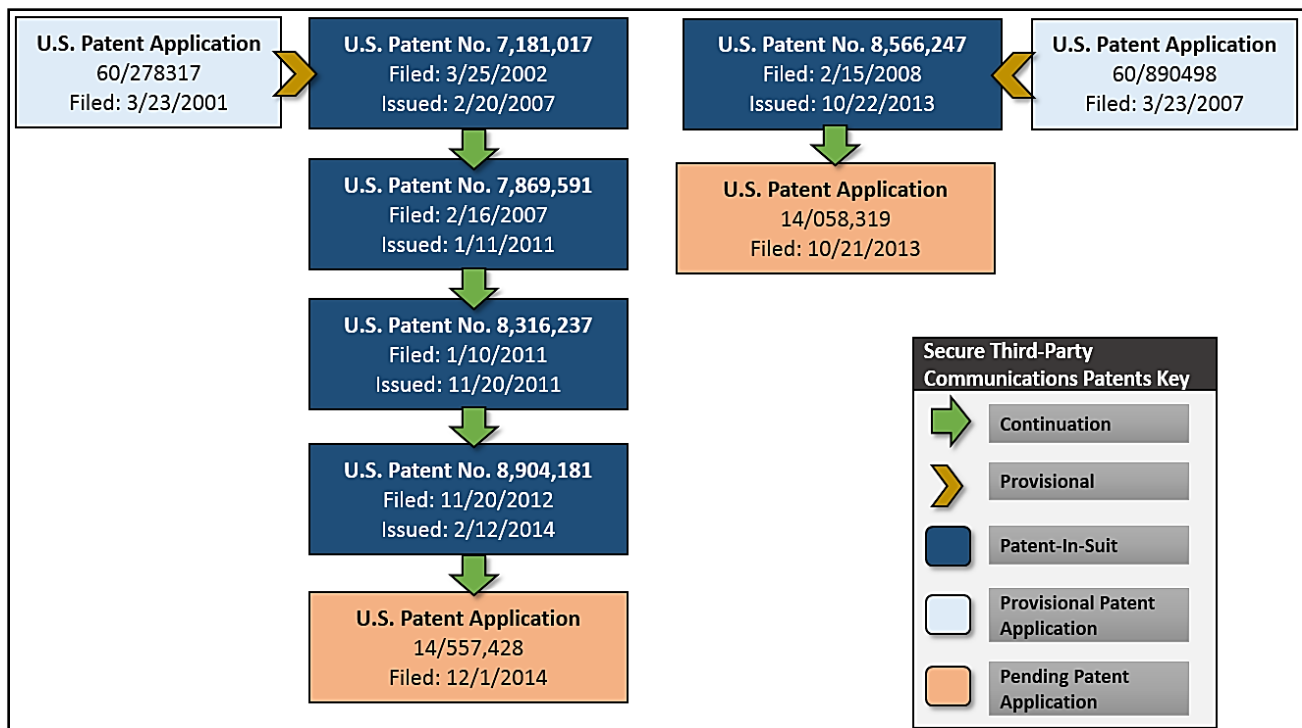
     4.   Over a decade after Dr. Nagel and his co-inventors conceived of the inventions

disclosed in the STPC patents, an Apple white paper described systems such as Dr. Nagel, Mr.

Felsher, and Mr. Hoffberg's secure third party communications system as "innovative" and a

"leap forward."

---

[1] St. Luke's STPC patents are in two patent families claiming priority to U.S. Patent Applications
60/278,317 and 60/890,498.

> We thought about the security hazards of the desktop environment, and established a new approach to security in the design of iOS. We developed and *incorporated innovative features that tighten mobile security* and protect the entire system by default. As a result, iOS is a major leap forward in security for mobile devices.

iOS SECURITY - WHITE PAPER 4 (February 2014) (emphasis added).

5.   Tim Cook, Apple's Chief Executive Officer, has repeatedly stated that the use of encryption technologies is central to Apple's business, particularly where data is stored in the "Cloud."

> We don't read your emails, we don't read your messages, we find it unacceptable to do that. I don't want people reading mine! […] We have designed Apple Pay purposely so that we don't know where you buy something, how much you pay for it, what you bought. We don't want to know any of that.

Warum ich mich den Deutschen so nah fühle, BILDE-ZEITUNG INTERVIEW, March 2015 (Mr. Cook went on to describe the importance of secure communications in the context of email hacking: "If Snowden did anything for us at all, then it was to get us to talk more about these things.").

6.   Mr. Felsher is the inventor of the '368 patent, the '941 patent, and U.S. Patent Nos. 7,805,377 ("the '377 patent"), 8,380,630 ("the '630 patent"), and 8,600,895 ("the '895 patent") (collectively, "Information Record Infrastructure Patents" or "IRI patents"). The IRI patents have been cited by over 970 United States patents and patent applications as prior art before the United States Patent and Trademark Office.

7.   The IRI patents disclose systems and methods for distributing and granting access to data where data is stored in multiple external computer databases. The IRI patents address the difficult problem of authorizing access to protected information records where authorization will depend on the access privileges of the user.

8.   The below diagram shows the IRI patent family tree, a pending IRI patent application, and the IRI patents Apple is accused of infringing.
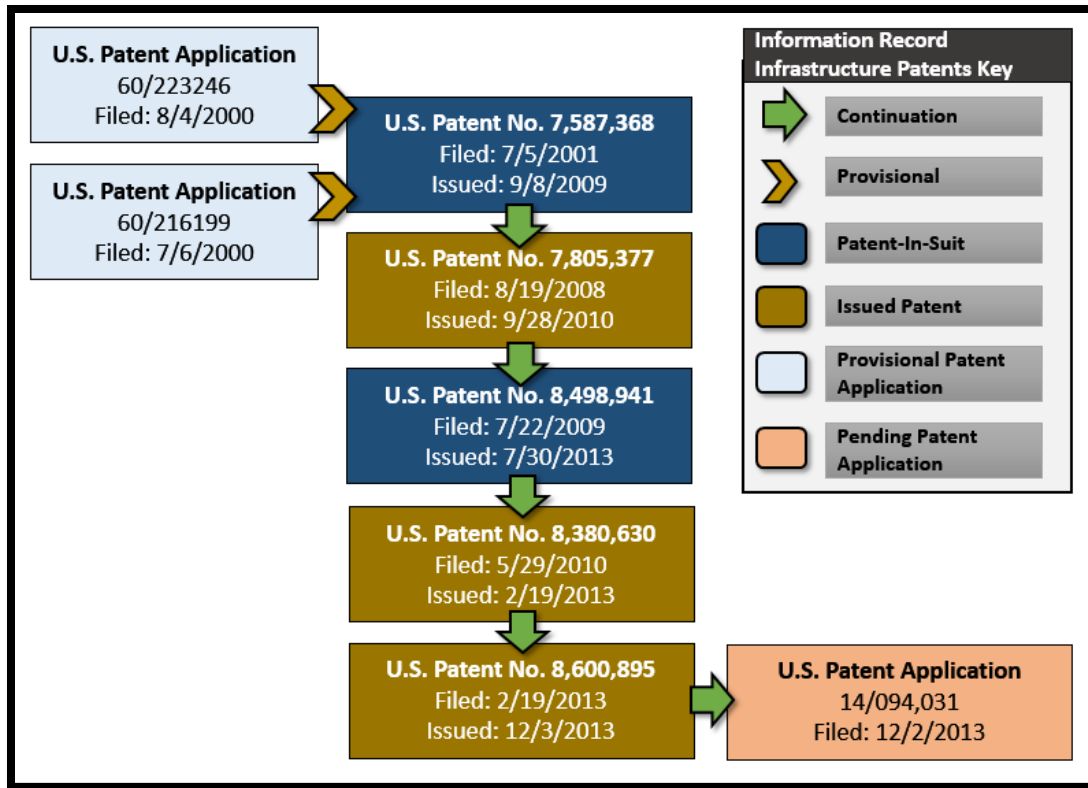
THE INVENTORS' LANDMARK SECURE COMMUNICATION SYSTEMS

9.   Mathematician Dr. Robert Nagel, the named inventor of five patents-in-suit, pioneered development of large-scale computer-based data distribution systems. In the 1970s Dr. Nagel developed some of the first computer systems for distributing encrypted data over computer networks. Dr. Nagel is the named inventor of twenty-three United States Patents. Dr. Nagel's patents have been cited thousands of times by various companies, including Apple. Later in life, Dr. Nagel founded two publicly traded companies, and served as a representative to the United Nations.

10.   In 1975, Dr. Nagel developed a system harnessing burgeoning microprocessor power to broadcast stock prices and related data over coaxial cable and telephone networks. Dr. Nagel's patented system was the foundation of Reuters's high-speed transmission technologies for distributing real-time market information.

> Computer power behind the new information system is provided by a Digital Equipment Corp. PDP-8E with 32K memory and a multiprocessor system consisting of one PDP-11/35 with 64K memory and 2 PDP-11/50s, each with 96K memory.
> The system was developed by Robert H. Nagel of IDR. Another patent for the high-speed transmission technique is expected to be issued shortly.

REUTERS GETS NEWS SYSTEM PATENT, COMPUTERWORLD at 36, April 23, 1975 (describing Dr. Nagel's development of one of the first terminals for displaying real-time stock market data).[2]

11.   The data distribution system developed by Dr. Nagel in the mid-1970s was commercialized by Reuters and allowed the rapid transmission of market and news information over coaxial cable and telephone lines.[3]


IMAGE OF THE DEC PDP-11/50 SYSTEM, COLUMBIA UNIVERSITY COMPUTING HISTORY ARCHIVE (circa 1976), http://www.columbia.edu/cu/computinghistory/ (showing an installed PDP-11/50 device that was a component in Dr. Nagel's data distribution system).

---

[2] *See* U.S. Patent Nos. 3,875,329, which issued on April 1, 1975. Dr. Nagel's work at IDR, Inc. (a subsidiary of then Reuters Group PLC) lead to the development of U.S. Patent Nos. 3,889,054; 4,042,958; 4,064,494; 4,120,003, 4,135,213; and 4,148,066. These patents have been cited in over 830 patent applications and issued patents of companies including Cisco Technology, Inc., Sony Corporation, Intel Corporation, etc.

[3] REUTERS TECHNICAL DEVELOPMENT CHRONOLOGY 1975-1979, THE BARON, July 13, 2015), http://thebaron.info/archives/technology/reuters-technical-development-chronology-1975-1979.

12.   Reuters sold thousands of information systems modeled on Dr. Nagel's patented inventions.[4] Hundreds of companies including IBM, Intel, and Xerox cite Dr. Nagel's groundbreaking inventions described in his patents as relevant prior art in their own patents.[5]
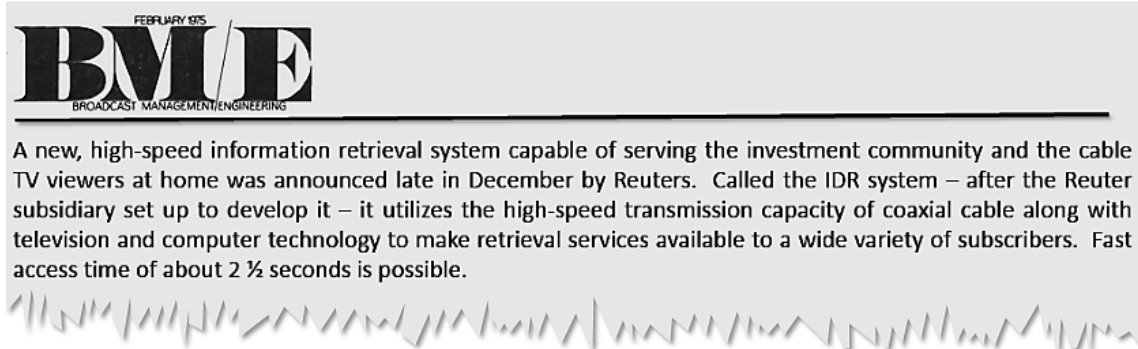
REUTERS ANNOUNCES RETRIEVAL SYSTEM FOR CABLE TV SUBSCRIBERS, BROADCAST MANAGEMENT/ENGINEERING MAGAZINE at 9, February 1975.

13.   In the 1990s, Dr. Nagel was the Chief Technology Officer of eSecure Docs, Inc., Founder of Digits Corporation, and Executive Vice President and Chief Technology Officer of InfoSafe Systems, Inc.[6] Publications including Fortune Magazine and ComputerWorld

---

[4] REUTERS TECHNICAL DEVELOPMENT CHRONOLOGY 1975-1979, THE BARON, July 13, 2015), http://thebaron.info/archives/technology/reuters-technical-development-chronology-1975-1979 (More than 10,000 units are eventually produced. It revolutionizes the Monitor product financials and field staffing and provides valuable cash flow for IDR.").

[5] PROCEEDINGS OF THE DIGITAL EQUIPMENT USERS SOCIETY, DIGITAL EQUIPMENT CORPORATION PROCEEDINGS Vol. 3 Issue 1 at 1 (1977) ("Reuters has developed a network to assist stock and commodity brokers and foreign exchange dealers by giving them the latest prices and rate of exchange via terminals in this book."); ANNUAL REVIEW OF INFORMATION SCIENCE AND TECHNOLOGY, AMERICAN SOCIETY OF INFORMATION SCIENCE, AMERICAN DOCUMENTATION INSTITUTE Vol. 12 at 223 (1977) ("Reuters provides the user with a 1.2 Kbps leased connection to the nearest network processor or multiplexor. The Monitor user configuration is a Digital Equipment Corporation PDP 8 with up to three display units."); REUTERS BLENDS CATV & COMPUTER SKILLS IN NEWS RETRIEVAL SYSTEM, DATA PROCESSING DIGEST at 12 (1975) ("Reuters has introduced in New York a high-speed information retrieval system for the investment community. The system was developed by Information Dissemination and Retrieval, Inc. (IDR), a Reuters subsidiary, and uses the high-speed transmission capacity of coaxial cable with television and computer technology.").

[6] In addition to his work in private industry, Dr. Nagel served as a consultant to the Defense Advanced Research Projects Agency ("DARPA"), responsible for the development of emerging technologies used by the U.S. Department of Defense. Dr. Nagel was a designer of the Navy's Tactical Air Navigation System ("TACAN") and assisted in the development of the nuclear reactor that powers the Navy's Seawolf class of nuclear submarines. Dr. Nagel was also the developer of the Hot Well Liquid Level Control system that is a part of the control system of the nuclear power plant aboard the Seawolf, Defender and other submarines.

described Dr. Nagel as a "noted computer scientist" for his groundbreaking work[7]—work that led to the inventions disclosed in the patents-in-suit.

> The technology Nagel designed at InfoSafe Systems, Inc., won the Seybold Award for Excellence as the "most innovative product of the year." His work in high technology received major press coverage in such publications as Fortune, Forbes, and Business Week. He testified before Congress on the capabilities of a system he designed for NASDAQ.

Aliye Pekin Celik, OUR COMMON HUMANITY IN THE INFORMATION AGE: PRINCIPLES AND VALUES FOR DEVELOPMENT at 191 (2007).

14.   Following his development of groundbreaking electronic data distribution systems for Reuters, Dr. Nagel used his insights to develop the secure communications technologies that are used today by Apple and many of the world's largest corporations without attribution or compensation.

15.   Dr. Nagel foresaw the need for enabling secure communications between two parties wherein an intermediary performs a requisite function with respect to the transaction without requiring the intermediary to be trusted with respect to the private information or cryptographic keys for communicated information.

16.   Dr. Nagel's interest in developing secure systems for the provision of highly secure data was driven in part by his experience being totally blind.[8] Dr. Nagel recognized that the growing adoption of the Internet and increased computational power presented unique challenges to the security of medical records. Dr. Nagel also had the insight that the challenges presented in controlling access to secure medical records could be applied outside the context of

---

[7] *See* Rick Tetzeli, et al., *Fortune Checks Out 25 Cool Companies For Products, Ideas, And Investments*, FORTUNE MAGAZINE, July 11, 1994.

[8] Dr. Nagel served as a representative to the United Nations Committee that authored the International Convention on the Protection of the Rights of Dignity of Persons with Disabilities *See* Jan Jekielek, *Human Rights Panel Explores Implementation of Rights and Global Well-Being*, Epoch Times, December 3, 2010, http://www.cccun.net/cccun-12-2-10-eventepochtim.pdf ("Nagel, who is blind himself. He expounded on the remarkable accomplishment that is the Convention on the Rights of Persons with Disabilities, the 21st century's first U.N. human rights convention.").

medical records, with wide applicability to the security of data on networks where an intermediary could have access to secure information.

17.   The rise of cloud computing (the delivery of on-demand computing resources over a distributed network), has made Dr. Nagel and his co-inventors' insights uniquely valuable. Medical records, financial information, email messages, and other forms of electronic data are now placed on remote servers and accessed via a network by a diverse variety of users, under a diverse variety of circumstances.

18.   The inventions disclosed in the STPC patents address shortcomings in systems available at the time of the patents' conception—for example, the need for users in particular contexts, to access and/or modify data stored at or by an intermediary without allowing the intermediary to access an unencrypted version of the data.

19.   Prior art systems such as the "Micali Fair Encryption scheme do[] not . . . allow communications of a secret in which only one party gains access to the content, and in which the third party or parties and one principal operate only on encrypted or secret information." '237 patent, col. 2:40-44.
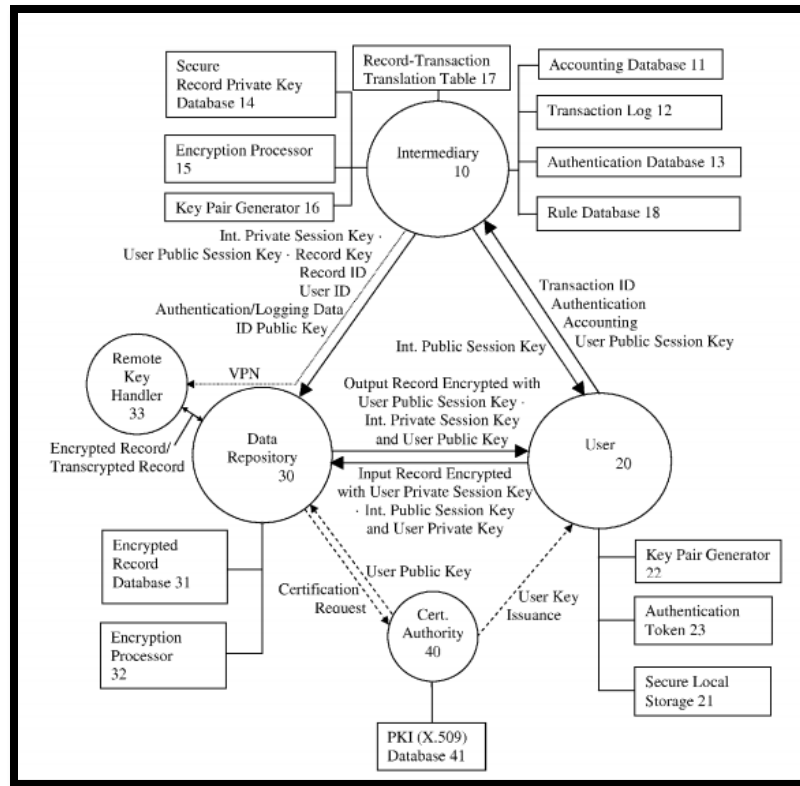
'237 Patent Fig. 1.

20.   Dr. Nagel worked with Steven Hoffberg and David P. Felsher to develop the systems and methods disclosed in the STPC patents. The inventions taught in these patents relate to the secure transmission of data—for example, wherein an intermediary performs a requisite function with respect to a secure data transmission without requiring the intermediary to be trusted with the private, secure contents of the transmission and/or without requiring the intermediary to have access to the cryptographic keys required to access the protected information. The STPC patented systems and methods employ secure cryptographic schemes, which reduce the risks and liability of unauthorized disclosure of private information as it travels across a network.

21.   Mr. Hoffberg holds a Master of Science degree from the Massachusetts Institute of Technology and an advanced degree in electrical engineering from Rensselaer Polytechnic Institute. Mr. Hoffberg is a named inventor on sixty-seven patents in the fields of telematics, wireless ad hoc networking, image and audio signal processing, and cryptography. Mr. Hoffberg

9

also spent three years in the University of Connecticut Medical School Medical Doctorate Program.

22.   Mr. Felsher is an appellate attorney, health care activist, and inventor. After graduating from MIT with a Bachelor of Science Degree in Chemistry, Mr. Felsher went on to earn an MBA from the Wharton School of Business of the University of Pennsylvania and a J.D. from Fordham Law School.[9] Mr. Felsher has served as counsel to the Association of American Physicians and Surgeons, Inc.

23.   The STPC patents have been cited in over 550 United States patents and published patent applications as prior art before the United States Patent and Trademark Office.[10] Companies whose patents cite the Secure Third-Party Communication Patents include:

- Microsoft Corporation
- Nokia Corporation
- Apple, Inc.
- International Business Machines Corporation
- Massachusetts Institute Of Technology
- Ncr Corporation
- Netapp, Inc.
- Adobe Systems Incorporated
- American Express Travel Related Services Company, Inc.
- AT&T Intellectual Property LLP
- Canon Kabushiki Kaisha
- Hytrust, Inc.
- Cisco Technology, Inc.
- Intuit Inc.
- Cloudera, Inc.
- Novell, Inc.
- Google Inc.
- Teradata Us, Inc.
- Mitsubishi Electric Corporation
- Texas Instruments Inc.
- Unitedhealth Group Incorporated
- Fujitsu Limited
- Hewlett-Packard Development Company, L.P.
- Verizon Patent and Licensing Inc.
- Visa U.S.A. Inc.
- Western Digital Technologies, Inc.

---

[9] During his legal career, Mr. Felsher has been counsel of record on seventeen briefs to the United States Supreme Court.

[10] The 550 forward citations to the Secure Third-Party Communication Patents do not include patent applications that were abandoned prior to publication in the face of the Secure Third-Party Communication Patents.

- Xerox Corporation
- Yahoo! Inc.
- Koninklijke Philips Electronics, N.V.
- Zynga Inc.
- Square, Inc.
- Sprint Communications Company L.P.
- Sony Corporation
- Siemens Aktiengesellschaft
- Sharp Laboratories of America, Inc.
- Sap AG
- EMC Corporation
- Samsung Electronics Co., Ltd.
- Ricoh Co., Ltd.
- Red Hat, Inc.
- Panasonic Corporation
- Broadcom Corporation
- Oracle International Corporation

24.   The inventions taught in the STPC patents relate to the encryption of data passed through an intermediary and have been recognized by Apple as important and valuable: "iCloud Keychain encryption keys are created on your devices, and Apple can't access those keys. Only encrypted keychain data passes through Apple's servers, and Apple can't access any of the key material that could be used to decrypt that data."[11]

25.   The adoption of secure encryption technologies was critical to Apple's current success. An April 2008 article in PC Magazine describes Apple's struggles with developing sufficient encryption for data passed over a computer network by intermediaries:

> Macs are banned from many government departments ***because there aren't any 'approved' applications to encrypt them***. So why doesn't Apple CEO Steve Jobs do something about it? In the US last week, The National Health Institutes banned MacBooks from being used by staff because they lack an approved encryption tool to protect client information, according to a report in *InformationWeek*.

Liam Tung, *Nobody Protect Macs, Not Even Steve Jobs*, ZDNET.COM WEBSITE, April 15, 2008 (emphasis added).

---

[11] ICLOUD KEYCHAIN, ICLOUD SECURITY AND PRIVACY OVERVIEW, last visited September 2, 2015, https://support.apple.com/en-us/HT202303

26.   The IRI patents have been cited by over 970 United States patents and patent

applications as prior art before the United States Patent and Trademark Office.[12] Companies

whose patents cite the IRI patents include:

- Bank Of America Corporation
- Siemens Medical Solutions Health Services Corporation
- AthenaHealth, Inc.
- Robert Bosch Gmbh
- Thompson Reuters (Healthcare) Inc.
- Northrop Grumman Information Technology, Inc.
- McKesson Corporation
- Lockheed Martin Corporation
- Sandisk Technologies Inc.
- Intel Corporation
- Greenway Medical Technologies, Inc.
- Medtronic, Inc.
- Sybase, Inc.
- General Electric Company
- Epic Systems Corporation
- Allscripts Software, Llc
- Ebay, Inc.
- 3Com Corporation
- Oracle International Corporation
- Intuit Inc.
- Gemalto Sa
- Adobe Systems Incorporated
- Koninklijke Philips Electronics N.V.
- Electronic Data Systems Corporation
- American Express Travel Related Services Company, Inc.
- Google Inc.
- Apple, Inc.
- Mcafee, Inc.
- Hewlett-Packard Development Company L.P.
- EMC Corporation
- Blackboard Inc.
- AT&T Intellectual Property LLP
- Cerner Innovation, Inc.
- Cisco Technology, Inc.
- Citrix System, Inc.
- International Business Machines Corporation

THE PARTIES

27.   Tyler, Texas-based St. Luke is committed to advancing the current state of

innovation in the field of data encryption technologies for secure communications over a

---

[12] The 970 forward citations to the IRI Patents and their related patent applications do not include
patent applications that were abandoned prior to publication in the face of the IRI Patents.

distributed network. In addition to the ongoing efforts of Messrs. Felsher and Hoffberg, St. Luke employs a resident of Tyler, Texas as a Technology Analyst. St. Luke is a Texas limited liability company with its principal place of business at 719 West Front Street, Suite 247, Tyler, Texas 75710.

28.   St. Luke is a small, Texas-based company. St. Luke depends on patent protection to effectively license its innovative technologies and build its business. Like Defendant Apple, St. Luke relies on its intellectual property. Apple's Chairman and President, Tim Cook, explained the importance of protecting Apple's intellectual property:

> We like competition--as long as our competitors don't rip off our IP. And we're going to go after anyone who does. I'm not talking about any particular company, but we are ready to suit up and go against anyone. ***We will not stand for having our IP ripped off***, and we will use every weapon at our disposal....

John Paczkowski, *Apple COO [Tim Cook]: "Will Not Stand For Having Our IP Ripped Off*, ALLTHINGSDIGITAL.COM, January 21, 2009 (emphasis added).

29.   On information and belief, Apple has asserted its patents in federal courts, including the Eastern District of Texas.[13]

---

[13] *See Affinity Labs of Tex., LLC v. Apple, Inc.*, 2009 WL 7376918, *4 (E.D. Tex. Aug. 25, 2009) (describing Apple Computer's previous litigation); *Apple Computer, Inc. v. Creative Tech. Ltd. and Creative Labs Inc.*, Case No. 06-cv-149, Dkt. No. 1 (E.D. Tex. Filed July 19, 2006) (asserting infringement of U.S. Patent No. 7,046,230); *see also* Testimony from Apple's Corporate Representative in *VirnetX Inc. v. Apple Inc.*, Case No. 6:10-CV-417 (E.D. Tex. filed Aug. 10, 2011), Trial Tr., 11/02/12, 38:18-22; see also *id.* at 37:23-24 ("It's a pretty short flight, so it's not a big deal."). More recently, Apple, as majority owner of the Rockstar Consortium, filed a complaint in this District a year ago. *See Rockstar Consortium v. Google, Inc.*, Case No. 13-CV-893-JRG (E.D. Tex. filed Oct. 31, 2013). Apple filed suit against HTC in the District of Delaware across the continent. *See Apple, Inc. v. HTC, et al.*, 1:10-CV-0167 (D. Del. filed Mar. 2, 2010).

30.   On information and belief, Apple is a California corporation with its principal office at 1 Infinite Loop, Cupertino, California, 95014. Apple can be served through its registered agent, CT Corporation System, 1999 Bryan Street, Suite 900, Dallas, Texas 75201.

31.   On information and belief, Apple has offices in Texas where it sells, develops, and/or markets its products including:

- Apple developers integral to the accused products' infringing capabilities.
- Apple's Austin office is currently undergoing a $300 million expansion and growing from 3500 to 7000 employees.[14]
- Apple operated a patent licensing company in Plano, Texas through its majority-owned subsidiary Rockstar Consortium.
- The supplier of numerous Apple chips (via Samsung) is located in or near the Eastern District of Texas.

32.   According to Apple's website, Apple offers infringing products for sale throughout the United States and Canada, including in the Eastern District of Texas. Further, Apple advertises its infringing products throughout the Eastern District of Texas and claims financial benefits through its conducting of business in Texas, including: (1) accepting monies from the state of Texas relating to Apple's engagements with Texas entities;[15] (2) ongoing contracts with the state of Texas;[16] (3) Apple's agreement to be subject to the laws and

---

[14] Nicole Raney, *Apple Continues Massive Austin Expansion With New Acquisition*, AUSTINCULTUREMAP.COM, April 27, 2015, http://austin.culturemap.com/news/innovation/04-27-15-apple-expansion-offices-lease-southwest-austin-jobs/ ("The massive operations center and satellite office spaces are an extension of Apple's headquarters in Cupertino, California. In addition to providing overflow space for Apple's main hub, Austin houses Apple's hardware development and support teams.").

[15] *Apple in Texas: State of Texas Purchase Agreement(s),* APPLE WEBSITE, September 2015, http://www.apple.com/education/purchase/contracts/states/tx.html; *Texas Department of Information Resources: Apple Inc. Contract Overview*, TEXAS GOVERNMENT WEBSITE, September 2015, http://dir.texas.gov/View-Search/Contracts-Detail.aspx?contractnumber=DIR-SDD-2068&keyword=apple.

[16] *DIR Contract No. DIR-SDD-2068*, STATE OF TEXAS DEPARTMENT OF INFORMATION RESOURCES CONTRACT FOR PRODUCTS AND RELATED SERVICES ORACLE AMERICA, INC. (2015), http://publishingext.dir.texas.gov/portal/internal/contracts-and-services/Contracts/DIR-SDD-2068%20Contract.pdf.

jurisdiction of Texas;[17] (4) Apple's certification that it is licensed to conduct business in Texas;[18] (5) Apple's assent to Texas insurance liability;[19] and (6) Apple's agreement (in prior contracts with the state of Texas) to make documentation available to residents of Texas.[20]

33.   On information and belief, Apple has acquired companies relevant to the accused products, including Intrinsity, Inc., which is based in Texas.

JURISDICTION AND VENUE

34.   This action arises under the patent laws of the United States, Title 35 of the United States Code. Accordingly, this Court has exclusive subject matter jurisdiction over this action under 28 U.S.C. §§ 1331 and 1338(a).

35.   Upon information and belief, this Court has personal jurisdiction over Apple in this action because Apple has committed acts within the Eastern District of Texas giving rise to this action and has established minimum contacts with this forum such that the exercise of jurisdiction over Apple would not offend traditional notions of fair play and substantial justice. Defendant Apple, directly and/or through subsidiaries or intermediaries (including distributors, retailers, and others), has committed and continues to commit acts of infringement in this District by, among other things, offering to sell and selling products and/or services that infringe the patents-in-suit. Moreover, Apple is registered to do business in the State of Texas, and has appointed CT Corporation System, 1999 Bryan Street, Suite 900, Dallas, Texas 75201, as its agent for service of process.

---

[17] *Id*. at Appendix A § F ("The laws of the State shall govern the construction and interpretation of the Contract.").

[18] *Id*. at Appendix A § D ("Vendor [Apple] and its Order Fulfiller shall be authorized and validly existing under the laws of its state of organization, and shall be authorized to do business in the State of Texas.").

[19] *Id.* at Appendix A § N ("licensed in the State of Texas, and authorized to provide the corresponding coverage").

[20] *Id.* at Appendix A § V(1) ("Pursuant to S.B. 1368 of the 83rd Texas Legislature, Regular Session, Vendor is required to make any information created or exchanged with the State pursuant to this Contract, and not otherwise excepted from disclosure under the Texas Public Information Act, available in a format that is accessible by the public at no additional charge to the State.").

36.   Venue is proper in this district under 28 U.S.C. §§ 1391(b)-(d) and 1400(b). Defendant Apple is registered to do business in Texas, and upon information and belief, has transacted business in the Eastern District of Texas and has committed acts of direct and indirect infringement in the Eastern District of Texas.

TECHNOLOGY BACKGROUND

37.   Advances in computational power and the explosive growth of the Internet have led to the development of secure encryption systems and information record management systems that enable secure communications between two or more computers on a network where the data that is sent and/or processed by an intermediary without access to the plaintext data.

- *The STPC patents* teach specific computer based encryption systems, including systems that use composite key asymmetric cryptographic algorithms to avoid substantially revealing plaintext data during intermediate processing.
- *The IRI patents* teach specific computer based systems and methods, including systems for electronically structuring and controlling access to protected data in a plurality of external databases.

A.   Secure Third Party Communications Patents

38.   Apple prizes systems that provide secure third party communications through an intermediary. Recently, Apple has come under criticism for providing end-to-end encryption as an intermediary, such that protected third-party electronic information on Apple's intermediary servers is not viewable to Apple in unencrypted form. In a June 2015, speech delivered to the Electronic Privacy Center, Tim Cook, Apple's CEO stated:

> Removing encryption tools from our products altogether, as some in Washington would like us to do, would only hurt law-abiding citizens who rely on us to protect their data. The bad guys will still encrypt, it's easy to do and readily available.

Matthew Panzarino, *Apple's Tim Cook Delivers Blistering Speech on Encryption, Privacy,* TECHCRUNCH WEBSITE, June 2, 2015, http://techcrunch.com/2015/06/02/apples-tim-cook-delivers-blistering-speech-on-encryption-privacy/#.wsy2vn:ybuV.

39.   In a 2014 earnings call, Tim Cook tied the financial success of Apple to Apple's

use of strong encryption and, specifically, Apple's use of end-to-end encryption which prevents

Apple from decrypting data that is stored or sent through its servers.

> Tim Cook: We've also communicated and demonstrated our commitment to respecting and protecting users' privacy with strong encryption and strict policies that govern how our data is handled.

APPLE Q4 2014 EARNING CALL TRANSCRIPT, October 20, 2014,
http://seekingalpha.com/article/2576865-apples-aapl-ceo-tim-cook-on-q4-2014-results-earnings-call-transcript

40.   Apple's competitors such as Microsoft and Oracle have confirmed the importance

and value of encryption systems that protect data in the Cloud. Brendon Lynch, Chief Privacy

Officer at Microsoft described the importance that Microsoft places on secure encryption in the

cloud:

> We share the same concerns as our customers do around government surveillance.
> We know that customers will not use technology that they do not trust that is what
> people should know about our [Microsoft's] approach to this . . . we're
> implementing strong encryption right throughout our services to ensure that
> governments can only access data by lawful means."

Brendon Lynch, *Microsoft Privacy and Compliance in the Cloud*, TRUSTWORTHY COMPUTING -
VIDEO TRANSCRIPT, January 9, 2015, https://www.youtube.com/watch?v=q5rwwQBTJxo

41.   Vipin Samar, Vice President of database security product development at Oracle

states in a 2014 press release that, "As regulations worldwide increasingly call for more data to

be encrypted, organizations need a centralized solution to securely manage all the encryption

keys and credential files in their data centers." The press release continued by pointing out the

importance of secure encryption in the cloud.

> and backup mechanisms. As organizations increasingly encrypt data at rest and on the network, securely managing all the encryption keys and credential files in the data center has become a major challenge.
>
> At the same time, organizations also need to comply with stringent regulatory requirements for managing keys and certificates. Many global regulations and industry standards call for audits demonstrating that keys are routinely rotated, properly destroyed, and accessed solely by authorized entities.

ORACLE CUSTOMERS SECURE CRITICAL ENCRYPTION KEYS WITH ORACLE KEY VAULT, ORACLE
PRESS RELEASE, August 7, 2014.

42.   Although secure third party encryption systems that protect access to data at an intermediary are offered by major corporations today, at the time the inventions disclosed in the STPC patents were conceived, no such systems existed.

43.   The claims in the STPC patents describe a solution that is unquestionably rooted in computer technology to overcome a problem specific to and characteristic of complex computer networks. Professor of Computer Science at Columbia University, Steven M. Bellovin[21] described in a 1996 academic article, contemporaneous to the development of the patents-in-suit (and cited on the face of the STPC patents) that the development of modern cryptography was a reaction to the rise of the Internet as a mass medium and concerns unique to the exchange of information over the Internet.

> In early 1994, CERT announced[1] that widespread password monitoring was occuring on the Internet. In 1995, Joncheray published a paper explaining how an eavesdropper could hijack a TCP connection [Jon95]. In mid-1998, there is still very little use of cryptography. Finally, though, there is some reason for optimism.
>
> A number of factors have combined to change people's behavior. First, of course, there is the rise of the Internet as a mass medium, and along with it the rise of Internet commerce. Consider the following quote from a popular Web site:

Steven M. Bellovin, *Cryptography and the Internet*, AT&T LABS-RESEARCH, Aug. 1998, Florham Park, New Jersey.

44.   Although encryption, in some form, has been an objective of individuals (and governments) for many years, the STPC patents are directed at solving problems that are unique to the realm of computers and specifically network cloud computing.

45.   The specific technologies disclosed and claimed in the STPC patents are discussed in detail below. However, the history of cryptography provides context for the inventions disclosed in the STPC patents and confirms that the patented inventions are limited to specific computer systems and methods addressing issues specific to modern computer networks.

---

[21] At the time Professor Bellovin authored the above referenced article he was a Fellow at AT&T Labs Research.

46.   ***Pre-Mechanical Encryption***. The origin of cryptography has been around since the reign of Pharaohs; however, the problems that "pre-silicon" societies faced were markedly different than those the patents-in-suit are directed at solving. The unique solutions taught by the patents-in-suit reflect that difference. In 1900 BC, Egyptian scribes developed a rudimentary form of cryptography that allowed the passing of messages written on papyrus. The key to unlocking the meaning of non-standard hieroglyphs (the encrypted message or cipher) was located in an inscription on the same document. Thus, a recipient of a message could decipher the meaning of the encoded message using the key transmitted with the message. This early form of encryption was susceptible to frequency analysis, a method utilizing the frequency that certain letters or symbols would be used.[22]

Alexander Stanoyevitch, INTRODUCTION TO CRYPTOGRAPHY WITH MATHEMATICAL FOUNDATIONS AND COMPUTER IMPLEMENTATIONS PRESS (2002).

47.   Over the following four millennia, the advance of cryptography was limited. In the mid-1400s, Leon Battista Alberti invented an encryption system using a mechanical device with sliding disks that allowed for various methods of substitution.[23] This is the base concept of

---

[22] NIGEL SMART, CRYPTOGRAPHY: AN INTRODUCTION 3RD EDITION 40 (2004) ([U]nderlying statistics of the language could be used to break the cipher. For example it was easy to determine which ciphertext letter corresponded to the plaintext letter *E*.").

[23] DAVID KAHN, THE CODE BREAKERS: THE STORY OF SECRET WRITING 125 (1967) (David Kahn calls Alberti "the father of western cryptography" based on his development of a device that had two copper disks that fit together. "Each one of them had the alphabet inscribed on it. After every few words, the disks were rotated to change the encryption logic, thereby limiting the use of frequency analysis to crack the cipher.")

a polyalphabetic cipher, which is an encryption method that switches through several substitution ciphers throughout encryption. Polyalphabetic substitution by rotating the discs to change the encryption logic limited the use of frequency analysis to crack the cipher. However, polyalphabetic substitution was susceptible to plain text attacks that would try various permutations of the code.

48.   ***Encryption in the Mechanical Age***. In the 1920s, electro-mechanical devices were developed that used electrical signals to perform rudimentary calculations that would encrypt messages. The Enigma machine developed by the German government at the end of World War I used mechanical devices to encrypt and decrypt messages. Germany's Enigma device used a set of codes that, when programed into a device, would generate an encrypted message. Ciphers generated by the Enigma could thus be decrypted if one had both possession of an Enigma device and the "crib" or the symmetric key that was used to program the device.[24] Alan Turing (among others) wanted a technique to break Enigma that did not rely on the key, which could (and frequently did) change.[25] Turing developed several ways of using Bayesian inference coupled with "the Bombe," an electromechanical device that could detect the setting for the Enigma.

---

[24] DAVID KAHN, , SEIZING THE ENIGMA: THE RACE TO BREAK THE GERMAN U-BOAT CODES, 1939-1943 (1991) (In 1941 the British were able to decrypt ciphers generated by the enigma machine by discovering that portions of weather reports (Short Weather Codes) transmitted by German Warships were the symmetric key. However, in the fall of 1941 the German cryptographers stopped using short Weather Codes as symmetric keys. Subsequently, Germany out of abundance of caution changed the configuration of the enigma machines.).

[25] DAVID LEAVITT, THE MAN WHO KNEW TOO MUCH: ALAN TURING AND THE INVENTION OF THE COMPUTER (2006) (Turing settled on a known plaintext attack, using what was known at the time as a "crib." A crib was a piece of plaintext that was suspected to lie in the given piece of cipher text. The methodology of this technique was to form a given piece of cipher text and a suspected piece of corresponding plaintext to first deduce a so-called "menu." A menu is simply a graph, which represents the various relationships between cipher text and plaintext letters. Then the menu was used to program an electrical device called a Bombe.).
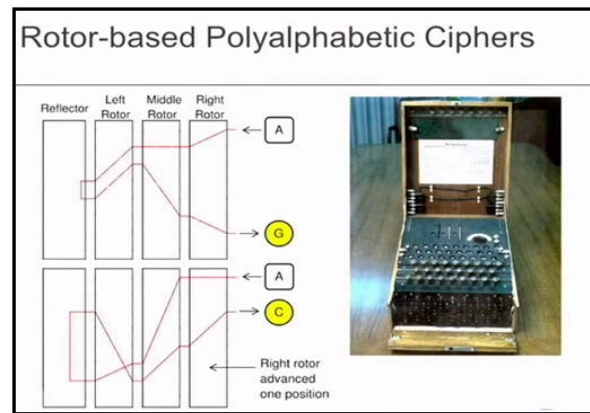
Steve Weis, THEORY AND PRACTICE OF CRYPTOGRAPHY 9:23 (November 2007) (image of the Enigma machine).

49.   ***The Development of Public Key Encryption***. Prior to 1976 (roughly three decades before the patents-in-suit issued), the only method of encryption was use of a symmetric key. Egyptian Ciphers, Polyalphabetic Encryption, and the Enigma Machine relied on a sender and receiver sharing the same key (a symmetric key). The advent of computer networks and the increasing computational power of computers spurred the invention of a cryptographic system specifically tailored toward encrypting and decrypting electronic messages communicated using a computer.

50.   In a 1976 paper, cited on the face of the STPC patents, Whitfield Diffie and Martin Hellman proposed the notion of *public-key* (frequently, and more generally, called *asymmetric key*) cryptography in which two different but mathematically related keys are used—a *public* key and a *private* key. Systems that utilize *public key* encryption were developed specifically to address problems unique to computer networking. Public key encryption at the time of the invention of the STPC patent technologies was not a long-held view, nor a technology that simply amounted to taking something and "doing it on a computer." The introduction to Diffie and Hellman's paper makes clear that public key systems were specific to computer networking.

21

> This paper deals with new problems which arise in the application of cryptography to computer communication systems with large numbers of users. Foremost among these is the key distribution problem. We

Diffie, et al., in *Multiuser Cryptographic Techniques*, AFIPS--CONFERENCE PROCEEDINGS, Vol. 45 at 109 (1976).

51.   A public key system contains two keys (numbers) so that calculation of one key (the 'private key') is computationally infeasible from the other (the 'public key'), even though they are necessarily related. Instead, both keys are generated secretly, as an interrelated pair. Public key encryption offered a novel mechanism for allowing two parties to share data over a network.

52.   The development of Diffie and Hellman's first public key system was directly motivated by the need to protect stored or transmitted data on a modern computer network.

> In a computer network with a large number of users, cryptography is often essential for protecting stored or transmitted data. While this application closely resembles the age old use of cryptography to protect military and diplomatic communications, there are several important differences which require new protocols and new types of cryptosystems. This paper addresses the multiuser aspect of computer networks and presents ways to preserve privacy of communication despite the large number of user connections which are possible.

Id.

53.   The Diffie-Hellman public key system illustrates the limitations present in systems for encrypting and decrypting information over a computer network contemporaneous to the STPC patents. The Diffie-Hellman system lacked the ability to enable the exchange of data between two parties through an intermediary where the intermediary would not have the ability to substantially decrypt the data. A 2005 paper (cited on the face of the STPC patents) described the limitations of the Diffie-Hellman system when conducting secure third party

communications. The paper also described a problem that the STPC patents solve as one that

had only recently been addressed:

> It was only recently that the problem has been formally addressed in the three-party model, where the server is considered to be a trusted third party (TTP). This is the same scenario used in the popular 3-party Kerberos authentication system. The main advantage of these systems is that users are only required to remember a single password, the one they share with a trusted server, while still being able to establish secure sessions with many users. ***The main drawback is the need of the trusted server during the establishment of these secure sessions.***

Michel Abdalla and David Pointcheval, *Interactive Diffie-Hellman Assumptions With Applications To Password-Based Authentication*, in PROCEEDINGS OF THE 9TH INTERNATIONAL CONFERENCE ON FINANCIAL CRYPTOGRAPHY AND DATA SECURITY (2005) (emphasis added).

54.   Another early encryption system developed for communications over a computer

network is a method of public-key encryption developed by Ron Rivest, Adi Shamir, and

Leonard M. Adleman, now generally referred to as "RSA." RSA is based on the use of two

extremely large prime numbers which fulfill the criteria for a "trap-door, one-way permutation."

Such a permutation function enables the sender to encrypt the message using a non-secret

encryption key, but does not permit an eavesdropper to decrypt the message through crypto-

analytic techniques within an acceptable period of time. This is because, for a composite number

composed of the product of two very large prime numbers, the computational time necessary to

factor this composite number is unacceptably long. A brute force attack requires a sequence of

putative keys to be tested to determine which, if any, is appropriate. A brute force attack

requires a very large number of iterations. The number of iterations increases exponentially with

the key bit size, while the normal decryption generally suffers only an arithmetic-type increase in

computational complexity.

55.   Like the Diffie-Hellman system, RSA was developed specifically to address

problems with sending and receiving encrypted information over a computer network. The

original RSA patent (cited on the face of the STPC and IRI patents) describes the use of public

key encryption as directed toward a computer network.

> With the development of computer technology, the transfer of information in digital form has rapidly increased. There are many applications, including electronic mail systems, bank systems and data processing systems, where the

> transferred information must pass over communications channels which may be monitored by electronic eavesdroppers.

U.S. Patent No. 4,405,829, col. 1:14-20.

56.   Academic articles from creators of the RSA system make clear that the use of

public key encryption is specific to problems unique to computer networks.

> [W]e present a sketch of how a computer system might be modified to solve the problem of performing operations on encrypted data securely. . . All sensitive data in main memory, in the data bank files, in the ordinary register set, and on the communications channel will be encrypted.   During operation, a load/store instruction between main memory and the secure register set will automatically cause the appropriate decryption/encryption operations to be performed.

Ronald L. Rivest, Leonard Adleman, and Michael L. Dertouzos, *On Data Banks and Privacy Homomorphisms*, IN ON DATA BANKS AND PRIVACY HOMOMORPHISMS 169 (1978).

57.   The RSA system illustrates limitations in encryption technologies that preceded

the STPC patents. RSA provided a mechanism for exchanging data between two parties but did

not disclose the use of an untrusted intermediary when data was exchanged between two parties.

A 1998 article contemporaneous to the development of the STPC patents (and cited on the face

of the STPC patents) describes this as a limitation in the RSA system and other systems known

at the time.

> We point out that classic techniques of secret sharing [14] are inadequate in this scenario. Secret sharing requires one to reconstruct the secret at a single location before it can be used, hence introducing a single point of failure. The technique described above of sharing the secret key such that it can be used without reconstruction at a single location is known as *Threshold Cryptography*. See [9] for a succinct survey of these ideas and nontrivial problems associated with them.
>
> An important question left out of the above discussion is key generation. Who generates the RSA modulus N and the shares d_1, d_2, d_3? Previously the answer

D. Boneh, J. Horwitz, *Generating A Product Of Three Primes With An Unknown Factorization*, in PROC. OF THE THIRD ALGORITHMIC NUMBER THEORY SYMPOSIUM (ANTS) 237 (1998).

58.   Silvio Micali's patents (U.S. Pat. Nos. 6,026,163 and 5,315,658; cited on the face

of the STPC patents) describe a split key, or so-called "fair" cryptosystem, designed to allow a

secret key to be distributed to a plurality of trusted entities, such that the encrypted message is

protected unless the key portions are divulged by all of the trusted entities. Thus, a secret key

may be recovered through cooperation of a plurality of parties. The Micali system provides that

the decryption key is split between a number (n) of trusted entities, meeting the following functional criteria: (1) The private key can be reconstructed given knowledge of all n of the pieces held by the plurality of trusted entities; (2) The private key cannot be guessed at all if one only knows less than all ($<n-1$) of the special pieces; and (3) For i-1, . . . n, the ith special piece can be individually verified to be correct.

59.   The Micali system does not allow communication of a secret in which only one party gains access to the content, and in which the third party or parties and one principal operate only on encrypted or secret information.

B.   The Value Of The Inventions Disclosed In The STPC Patents

60.   Executives at leading technology companies have described the value of specific encryption techniques as critical, lasting, and prominent. Chris Cicotte, a Cloud Architect at EMC, stated strong encryption technologies specific for networked computers "are a vital component of a strong security posture for any size organization, and it should be a standard offering within the cloud . . . . The threat landscape has already begun to evolve, and from an overall security perspective, we need to take a proactive approach by layering in technologies like encryption at every layer."[26] The development of secure communications systems and methods, such as the inventions taught in the STPC patents, was motivated by the unique problems created by the internet where secured data is often transmitted through untrusted intermediaries.

> Achieving secure communications in networks has been one of the most important problems in information technology. . . . If there is a private and authenticated channel between two parties, then secure communication between them is guaranteed. However, in most cases, many parties are only indirectly connected, as elements of an incomplete network of private and authenticated channels. ***In other words they need to use intermediate or internal nodes***.

Yvo Desmedt and Yongee Wang, *Perfectly Secure Message Transmission Revisited* at 502, Advances in Cryptology EUROCRYPT Vol. 2332 (2002) (emphasis added).

---

[26] Jude Chao, *Cloud Computing Demands Cloud Data Encryption*, ENTERPRISE NETWORKING PLANET WEBSITE, May 13, 2014, http://www.enterprisenetworkingplanet.com/netsecur/cloud-computing-demands-cloud-data-encryption.html.

61.   Companies such as Oracle Corporation, International Business Machines

Corporation, Hewlett-Packard Company, and Google, Inc., confirm the importance of providing

strong encryption systems that address the unique threats posed by moving data to the cloud.

> Once data is moved to the cloud, *it becomes vulnerable to a number of new threats* ranging from stolen administrator credentials to new hacking techniques. In addition, new legislation, such as the USA PATRIOT Act, is making it possible for competitors and governments to access data from cloud providers without the consent of the data owner. Many cloud providers thought they could achieve data sovereignty through locating cloud services in different jurisdictions, but this theory has been shaken by the subpoena classification ruling handed down recently in the U.S. federal court.

HP Atalla Cloud Encryption: Securing Data in the Cloud, HP TECHNICAL WHITE PAPER 2 (2014) (emphasis added).

> The need to secure data is driven by an expanding privacy and regulatory environment coupled with an increasingly dangerous world of hackers, insider threats, organized crime, and other groups intent on stealing valuable data. *The security picture is complicated even more by the rapid expansion of access to sensitive data via the Internet*, an unprecedented understanding of technology, increasing economic competition, and the push to achieve greater efficiencies through consolidation and cloud computing.

Oracle Database 12C Security And Compliance, ORACLE WHITE PAPER 2 (February 2015) (emphasis added).

> With rare exceptions, one of the most important assets for any company is its data. Your data may take the form of financial information, proprietary sales information, marketing information, healthcare information, intellectual property (IP), and more. Losing your data could negatively affect operations and potentially shut down your organization. . . . Cloud-aware applications create unique security challenges in that both Infrastructure as a Service (IaaS) providers and Platform as a Service (PaaS) providers make use of a shared-risk model.

Robi Sen, *Develop Secure Cloud-Aware Applications*, IBM DEVELOPER WORKS 2-3 (May 20, 2015).

> Business requirements, industry regulations, and government mandates increasingly dictate that your organization must secure electronic communications. Whether it is financial data, medical records, or proprietary corporate information, you simply must secure the delivery of sensitive content to its destination.

Google Message Encryption, GOOGLE APPLICATION SECURITY PAPER 1 (2008)

62.   Numerous academics have concluded the advent of cloud computing has created

challenges that are unique to cloud computing and these challenges require specific encryption

technologies that were previously unnecessary.

The growing demand for cloud computing stems from the need to securely store, manage, share and analyze immense amounts of complex data in many areas, including health care, national security and alternative energy. And although several companies have launched commercially available cloud systems, two areas still need significant improvements, [Dr. Bhavani] Thuraisingham said: the security mechanisms needed to protect sensitive data as well as the capability to process huge amounts of both geospatial data and what's known as semantic Web data.

Investment in Cloud Computing Research Pays Off, UT Dallas Computer Scientists Make Advances in Key Aspects of Growing Field, UNIVERSITY OF TEXAS AT DALLAS NEWS CENTER (April 19, 2011).[27]

Security is the most important challenge for cloud technology, as CSP's [Cloud Service Providers] have to protect the consumer's data from theft and ensure the consumer is not exploited. Consumers may be exploited from denial of service (DoS) attacks . . . ***They must also protect the data through the use of advanced encryption algorithms*** and ensure that their data centers are physically secure using advanced biometrics and many other authentication methods.

Sean Carlin & Kevin Curran, *Cloud Computing Technologies*, in INTERNATIONAL JOURNAL OF CLOUD COMPUTING AND SERVICES SCIENCE (IJ-CLOSER) Vol.1, No.2 at 59 (June 2012) (emphasis added).

The growth of computer networks and the opening that their interconnection brings, especially through Internet, mean that a great amount of information is traveling through network and ***crossing numerous intermediate systems. This results in the increase of the number of possible attacks and illegal operations***. . . . They should guarantee the identity of the communicating parties . . . the protection against unauthorized writing and, in some cases, unauthorized reading of transferred data. These services of authentication, nonrepudiation, integrity and confidentiality, respectively, can be provided using cryptosystems.

Natasha Prohic, *Public Key Infrastructures - PGP vs. X.509* at 1, in INFOTECH SEMINAR ADVANCED COMMUNICATION SERVICES (ACS) (2005) (emphasis added).

63.   On information and belief, contemporaneous to, and following conception of the

inventions disclosed in the STPC patents, academics, and businesses headquartered in Texas

---

[27] *See also* Kevin Hamlen et al., *Security Issues For Cloud Computing* at 39, INTERNATIONAL JOURNAL OF INFORMATION SECURITY AND PRIVACY Vol. 4(2) (April-June 2010) ("Because of the critical nature of the applications, it is important that clouds be secure. The major security challenge with clouds is that the owner of the data may not have control of where the data is placed."); Ryan Layfield, Murat Kantarcioglu, and Bhavani Thuraisingham, *Enforcing Honesty in Assured Information Sharing within a Distributed System*, IFIP WG 11.3 CONFERENCE ON DATABASE AND APPLICATIONS SECURITY (2007) ("The growing number of distributed information systems such as the internet has created a need for security in data sharing."); Safwan M. Khan and Kevin W. Hamlen, *AnonymousCloud: A Data Ownership Privacy Provider Framework in Cloud Computing* at 170, in PROCEEDINGS OF THE 11TH IEEE INTERNATIONAL CONFERENCE ON TRUST, SECURITY AND PRIVACY IN COMPUTING AND COMMUNICATIONS (June 2012) ("Revolutionary advances in hardware, middleware, and virtual machines over the past few years have elevated cloud computing to a thriving industry . . . . A significant barrier to the adoption of cloud services is customer fear of privacy loss in the cloud.").

actively entered the field of secure encrypted communications. Computer researchers at the University of Texas at Austin founded the Security Research Group. The University of Texas at Dallas founded the Data Security and Privacy Lab, a center for research on security issues raised by dissemination of data over computer networks.

64.   Texas based companies incorporated secure communications technologies into numerous products and many of these same companies cite STPC patents in their own patents. Texas based businesses that developed products incorporating secure communications technologies included: HP Enterprise Services, LLC of Plano, Texas; Texas Instruments, Inc. of Dallas, Texas; Rocksteady Technologies, LLC of Austin, Texas; Dell, Inc. of Round Rock, Texas; AT&T Intellectual Property whose inventors were based in various locations in Texas; Net.Orange, Inc. of Dallas, Texas; Futurewei Technologies, Inc. of Plano, Texas, etc.. The STPC patents are cited by at least 50 patents that were either initially assigned to or are currently assigned to entities headquartered in Texas.

1.   U.S. Patent No. 8,316,237

65.   U.S. Patent No. 8,316,237 (the "237 patent") entitled, System and Method for Secure Three-Party Communications, was filed on January 10, 2011 and claims priority to March 23, 2001. St. Luke is the owner by assignment of the '237 patent. A true and correct copy of the '237 patent is attached hereto as Exhibit A. The '237 patent claims specific methods and systems for securely transcrypting protected electronic information transmitted over at least one computer network from a first encrypted form to a second, different encrypted form substantially without intermediate decryption of the protected electronic information.

66.   The '237 patent has been cited by over 100 issued United States patents as relevant prior art. Specifically, patents issued to the following companies have cited the '237 patent as relevant prior art.

- Electronics and Telecommunications Research Institute (ETRI)
- NEC Corporation
- Disney Enterprises, Inc.
- WMS Gaming, Inc.
- Verizon Patent and Licensing, Inc.

- Microsoft Corporation.
- Netapp. Inc.
- NCR Corporation
- EMC Corporation
- AT&T Intellectual Property, L.P.
- Sony Corporation
- SAP AG
- Blackberry Limited
- Adobe Systems Incorporated
- Nippon Telegraph and Telephone Corporation
- Novell, Inc.
- Spring Communications L.P.
- Hytrust, Inc.
- International Business Machines Corporation
- Google, Inc.
- Kabushiki Kaisha Toshiba
- Panasonic Intellectual Property Management Co., Ltd.
- Zynga Inc.
- Certicom Corp.
- Wincor Nixdorf International Gmbh
- Oracle International Corporation
- Futurewei Technologies, Inc.
- Dell Products, L.P.
- Intuit Inc.

67.   The '237 patent claims a technical solution to a problem unique to computer networks – securely transmitting encrypted electronic information via an intermediary device, wherein the electronic information is cryptographically secure not only from outside attackers, but also from the intermediary.

68.   At the time of the inventions claimed in the '237 patent, securely processing, transmitting, and accessing protected electronic data in a massively distributed computing environment presented new and unique issues over the state of the art. As explained in the '237 patent: "Often, the nature of these communications protocols places the third party (or group of third parties) in a position of trust, meaning that the third party or parties, without access to additional information, can gain access to private communications or otherwise undermine transactional security or privacy." '237 patent, col. 2:13-17.

> Generating and protecting encryption keys while maintaining data availability has traditionally been a major barrier to implementing encryption, especially on an enterprise scale. Key management is complex and challenging, and often fails because issuance, storage, and renewing are difficult. ***Worse yet, lost keys can make important data permanently unrecoverable***.

Sustainable Compliance for the Payment Card Industry Data Security Standard, ORACLE WHITE PAPER 23 (July 2015) (emphasis added).

69.   Although the systems and methods taught in the '237 patent have been adopted by leading businesses today, at the time of invention, the technologies taught in the '237 patent claims were innovative and novel. "Typical public key encryption technologies, however, presume that a pair of communications partners seek to communicate directly between each other, without the optional or mandatory participation of a third party, and, in fact, are designed specifically to exclude third party monitoring." '237 patent, col. 2:56-61. Indeed, companies such as Oracle have recognized that, until recently, security for distributed systems was not a primary concern.

> - **Security was not a major issue, even for Oracle**
>   - Standard passwords (scott/tiger, system/manager, ...)
>   - Oracle standard users were installed and left open (though not at SAP!)
>   - There are some recommendations, but not much more.
>   - From Oracle9i, the issue of security was increasingly addressed by Oracle (DBCA: locking of default accounts,..., 10.2: CONNECT roles)

Andreas Becker, *High Security for SAP Data with Oracle Database Vault and Transparent Data Encryption*, ORACLE PRESENTATION 6 (2010).

70.   Further, the '237 patent claims improve upon the functioning of a computer system by allowing encrypted electronic data to be securely transmitted through an intermediary without the intermediary gaining substantial access to the unencrypted information. This improves the security of the computer system and allows it to be more efficient.[28] "Third parties,

---

[28] *See* Kevin Hamlen et al., *Security Issues For Cloud Computing* at 39, INTERNATIONAL JOURNAL OF INFORMATION SECURITY AND PRIVACY VOL. 4(2) (April-June 2010) ("The major security challenge with clouds is that the owner of the data may not have control of where the data is placed. . . . Therefore, we need to safeguard the data in the midst of untrusted processes."); Elana Ferrari and Bhavani Thuraisingham, *Security and Privacy for Web Databases and Services* at 17, PROCEEDINGS OF THE EDBT CONFERENCE (March 2003) ("very little work has been devoted to security"); Elisa Bertino et al.; *Selective and Authentic Third-Party Distribution of XML Documents* at 1263, IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, Vol. 16 No. 10 (October 2004) ("The most intuitive solution is that of requiring Publishers to be trusted with regard to the considered security properties. However, this solution could not always be feasible in the Web environment since large Web-based systems cannot be easily verified to be secure.").

however, may offer valuable services to the participants in a communication, but existing

protocols for involvement of more than two parties are either inefficient or insecure." '237

patent, col. 2:61-64. Studies have confirmed that the inventions disclosed in the '237 patent

improve the security of systems.

> ***Key management is a big concern with encryption, because the effectiveness of the solution ultimately depends on protecting the key***. If the key is exposed, the data being protected with the key is, essentially, exposed. Wherever the key is stored, it must be protected, and it should be changed on occasion. For example, if an administrator with access to a key leaves an organization, the key should be changed.

Tanya Baccam, *Transparent Data Encryption: New Technologies and Best Practices for Database Encryption*, SANS WHITE PAPER 3 (April 2010) (emphasis added).

71.   The '237 patent claims are not directed to a "method of organizing human

activity," "fundamental economic practice long prevalent in our system of commerce," or "a

building block of the modern economy." Instead, they are limited to a concretely circumscribed

set of methods and systems for transcrypting electronic information that is transmitted over a

computer network via an intermediary.

72.   The '237 patent claims are not directed at the broad concept/idea of "encrypting"

or "decrypting" information. Instead, they are limited to a concretely circumscribed set of

methods and systems for transcrypting electronic information that is transmitted over a computer

network via an intermediary. These methods and systems are technologies unique to the Internet

age.

73.   The inventive concepts claimed in the '237 patent are technological, not

"entrepreneurial." For example, transcrypting protected electronic information between a first

(e.g., server) encrypted form and a second (e.g., network) encrypted form without a substantial

intermediate representation of the information in decrypted form is a specific, concrete solution

to the technological problem of transferring encrypted information via an intermediary without

providing the intermediary substantial access to the information.

74.   Researchers have identified the problems the '237 patent is directed at solving

arise from new security challenges relating to cloud computing.

Deepak Panth, Dhananjay Mehta and Rituparna Shelgaonkar, *A Survey on Security Mechanisms*

> **Data Security:** Data security was the most important concern that had hindered the acceptance of the cloud computing initially. Storing and processing the data, running software, using CPU and virtual Machines on others' infrastructure were some serious concerns for the users initially. Data breach, data integrity and data loss are major security issues that posed threats to organization's data and software. Moreover, the multi-tenancy model and pooled computing resources over cloud have introduced new security challenges requiring new techniques to tackle with [4] [5] [6].

of Leading Cloud Service Providers, in INTERNATIONAL JOURNAL OF COMPUTER APPLICATIONS 98(1) at 34 (July 2014) (emphasis added).[29]

75.   The '237 patent claims are directed toward a solution rooted in computer technology and use technology unique to computers and computer networking to overcome a problem specifically arising in the realm of secure distributed computing. For example, claims of the '237 patent require transcrypting protected electronic information using one or more intermediary computing devices specially configured to yield a desired result—a result that overrides the routine and conventional sequence of events in electronic communications, even encrypted electronic communications.

76.   The '237 patent is directed to specific problems in the field of cryptography. In the "Background" section of the patent, the '237 patent explains that encryption systems use "keys," similar to passwords, to control how plaintext is encrypted and decrypted. '237 patent, col. 2:65–3:13. An encryption system thereby encrypts and decrypts information differently depending upon the key input. *Id.* Two common cryptanalytic attacks, linear and differential cryptanalysis, analyze large amounts of ciphertext (encrypted information) and different possible keys in order to eventually converge on the correct key and break the encryption. *Id.* at col. 3:1–3:13. Both attacks exploit the fact that some encryption systems use static keys to create the

---

[29] *See also* Vaibhav Khadilkar, Murat Kantarcioglu, and Bhavani Thuraisingham, *Secure Data Processing in a Hybrid Cloud* at 1-2, Computing Research Repository (CoRR) abs/1105.1982 (2011) ("The emergence of cloud computing has created a paradigm shift by allowing parallel processing of massive amounts of data. . . . [H]ow do users protect themselves from cloud service providers who may be able to access their data? This issue is related to data security and is relevant for users since their data is placed at the provider's site.").

ciphertext. *Id*. In other words, using the same key over and over gives an attacker more information to work with. The inventions of the '237 patent introduce several novel techniques to overcome these weaknesses and allow encrypted information to be securely transferred through an intermediary.

77.   The preemptive effect of the claims of the '237 patent are concretely circumscribed by specific limitations. For example, claim 1 of the '237 patent requires:

> A transcryption device, comprising:
>
> > an automated communication port configured to receive a first message representing an encrypted communication associated with a first set of asymmetric keys, to receive a transcryption key, and to transmit a second message representing the encrypted communication associated with a second set of asymmetric keys, the first and second sets of encryption keys being distinct;
> >
> > a memory; and
> >
> > an automated processor, configured to communicate through the automated communication port and with the memory, to receive the first message, receive the transcryption key, automatically transcrypt the first message into the second message, and to transmit the second message, wherein the automated processor does not store as a part of the transcryption any decrypted representation of the encrypted communication, and the transcryption key is employed without revealing any secret cryptographic information usable for decrypting the first message or the second message.

78.   The '237 patent does not attempt to preempt every application of the idea of encrypting electronic information transmitted over a computer network, or even the idea of encrypting electronic information transmitted over a computer network via an intermediary.

79.   The '237 patent does not preempt the field of secure third-party communications systems, or prevent use of alternative secure third-party communications systems. For example, the '237 patent includes inventive elements—embodied in specific claim limitations—that concretely circumscribe the patented invention and greatly limit its breadth. These inventive

elements are not necessary or obvious tools for achieving secure third-party communications, and they ensure that the claims do not preempt other techniques for secure communications.

80.   For example, the '237 patent describes numerous techniques for secure third-party communications that inform the invention's development but do not, standing alone, fall within the scope of its claims:

- Key Escrow. U.S. Pat. No. 6,009,177 to Sudia, relates to a cryptographic system and method with a key escrow feature that uses a method for verifiably splitting users' private encryption keys into components and for sending those components to trusted agents chosen by the particular users.

- Partitioning of Information Storage Systems. U.S. Patent No. 5,956,400 to Chaum, relates to partitioned information storage systems with controlled retrieval.

- Use of a Trusted Intermediary. U.S. Patent No. 6,161,181 to Haynes, describing secure electronic transactions using a trusted Intermediary; U.S. Patent No. 6,145,079 to Misty, describing secure electronic transactions using a trusted intermediary to perform electronic services.

- Split Key Storage. U.S. Patent No. 6,118,874 to Okamoto, teaching encrypted data using split storage key and system.

- Use of a Cryptographic File Labeling System. U.S. Pat. No. 5,953,419 to Lohstroh, disclosing cryptographic file labeling system for supporting secured access by multiple users.

- Computer Security Devices. U.S. Pat. No. 5,982,520 to Weiser, disclosing a personal storage device for receipt, storage, and transfer of digital information to other electronic devices; *see also* U.S. Pat. No. 5,991,519 to Benhammou; U.S. Pat. No. 5,999,629 to Heer; and U.S. Pat. No. 6,034,618 to Tatebayashi.

- Computer Network Firewalls And Agents. U.S. Pat. No. 6,061,798 to Coley, disclosed the use of an assigned proxy agent to verify the authority of an incoming request to access a network element indicated in the request. Once verified, the proxy agent completes the connection to the protected network element on behalf of the source of the incoming request; *see also* U.S. Pat. No. 6,023,762 to Dean, disclosing a data access and retrieval system which comprises a plurality of user data sources each storing electronic data signals describing data specific to a user, or enabling services selected by a user; an agent device which is configurable to select individual ones of the user data sources and

present selections of user data and service data to a set of callers who may interrogate the agent device remotely over a communications network; and U.S. Pat. No. 6,029,150 to Kravitz, disclosing a system and method of payment in an electronic payment system wherein a plurality of customers have accounts with an agent. Further, the patent lists thirty-three other patented systems involving Computer Network Firewalls that are not, standing alone, preempted by the inventions claimed in the patents-in-suit.

- Virtual Private Networks. As described in: U.S. Pat. No. 6,079,020 to Liu and U.S. Pat. No. 6,081,900 and twenty other patented systems involving virtual private networks that are not, standing alone, preempted by the inventions claimed in the patents-in-suit.

- Biometric Authentication. U.S. Pat. No. 5,193,855 to Shamos, disclosing the use of biometrics such as fingerprints to facilitate secure communications and identification of users. Further, the '237 lists 238 patented systems that use biometric authentication that are not, standing alone, preempted by the inventions claimed in the patents-in-suit.

81.   Although "[e]ncryption, in general, represents a basic building block of human ingenuity that has been used for hundreds, if not thousands, of years,"[30] the '237 patent does not claim, or attempt to preempt, "some process that involves the encryption of data for some purpose" (or similar abstraction).

82.   The '237 patent does not claim, or attempt to preempt, the performance of an abstract business practice on the Internet or using a conventional computer.

83.   The claimed subject matter of the '237 patent is not a pre-existing but undiscovered algorithm.

84.   The '237 patent claims systems and methods that "could not conceivably be performed in the human mind or pencil and paper."[31]

---

[30] *Paone v. Broadcom Corp.,* Case No. 15 CIV. 0596 BMC GRB, 2015 WL 4988279, at *7 (E.D.N.Y. Aug. 19, 2015) (*citing Fid. Nat'l Info. Servs., Inc.,* Petitioner, CBM2014-00021, 2015 WL 1967328, at *8 (Apr. 29, 2015) (both upholding the patent eligibility of patents directed toward encryption).

[31] *TQP Dev., LLC v. Intuit Inc.*, Case No. 2:12-CV-180-WCB, 2014 WL 651935, at *4 (E.D. Tex. Feb. 19, 2014) (finding claims directed to encryption to be patent eligible); *Paone v. Broadcom Corp.,* Case No. 15 CIV. 0596 BMC GRB, 2015 WL 4988279, at *7 (E.D.N.Y. Aug. 19, 2015); *see also Prism Technologies, LLC v. T-Mobile USA, Inc.*, 12-cv-124, Dkt. No. 428 at 7 (D. Neb. Sept. 22, 2015) (Finding on cross motions for summary judgment that patents directed at delivering resources over an untrusted network were patent eligible. "The problems addressed by Prism's claims are ones that 'arose uniquely in the context of the Internet.'").

85.   The '237 patent claims require the use of a computer system.

86.   The claims in the '237 patent require the modifying of data that has concrete and valuable effects in the field of secure third-party communications. By allowing an intermediary to receive secure information but not gain access to the unencrypted form of the information, the '237 patent improves the security of computer systems. Prior art systems that the '237 patent remedies enabled unauthorized "access to private communications or otherwise undermine[d] transactional security or privacy." Companies have described the use of encryption in the cloud as important to improve the security and functioning of systems.

> For many organizations, keeping data private and secure has also become a compliance requirement. Standards including Health Insurance Portability and Accountability Act of 1996 (HIPAA), Sarbanes-Oxley (SOX), Payment Card Industry Data Security Standard (PCI DSS), the Gramm-Leach-Bliley Act, and EU Data Protection Directives all *require that organizations protect their data at rest and provide defenses against threats*.

HP ATALLA CLOUD ENCRYPTION: SECURING DATA IN THE CLOUD, HP TECHNICAL WHITE PAPER 2 (2014).

87.   The '237 patent claims systems and methods not merely for transferring secure information over a computer network, but for making the computer network itself more secure. [32]

88.   The claimed invention in the '237 claims is rooted in computer technology and overcomes problems specifically arising in the realm of computer networks.

89.   The systems and methods claimed in the '237 patent were not a longstanding or fundamental economic practice at the time of the patented inventions. Nor were they fundamental principles in ubiquitous use on the Internet or computers in general. As just one

---

[32] Limitations in the prior art that the '237 patent was directed to solving included: computer systems where a "third party plays a requisite role in the transaction but which need not be trusted with access to the information or the cryptographic key" (*Id.*, col. 2:5-7): "[p]asswords may be written near access terminals (*Id.* col. 1:50-51);" "[s]ecurity tokens can be stolen or misplaced" (*Id.*, col. 1:51-52); "users may share supposedly secret information" (*Id.*, col. 1:52); and "unauthorized uses of the system" (*Id.*, col. 11:28). The '237 patent "allows the entity that transmits the information to be assured that the transmission will be secure, even with respect to a trusted third party, while ensuring that the intended recipient must cooperate with the intended third party." '237 patent, col. 8:48-52.

example, at the time the inventions disclosed in the '237 patent were conceived, the use of

asymmetric encryption keys was described by Oracle as "relatively new."[33]

> A Public Key Infrastructure (PKI) consists of protocols, services, and standards supporting applications of public key cryptography. ***Because the technology is still relatively new***, the term PKI is somewhat loosely defined.

INTRODUCTION TO THE SSL TECHNOLOGY, ORACLE DOCUMENTATION (February 1, 2001), http://docs.oracle.com/cd/E53645_01/tuxedo/docs12cr2/security/publickey.html

90.   The asserted claims do not involve a method of doing business that happens to be

implemented on a computer; instead, the '237 patent teaches changing data in a way that will

affect the communication system itself, by making it more secure. The security challenges that

the '237 patent is directed at overcoming were new and unique to distributed networks, as

confirmed in a recent paper from Accenture Services Pvt. Ltd.: "The unprecedented growth of

cloud computing has created new security challenges. The problem is ever more complex as

there is a transition from traditional computing to a service-based computing."[34]

91.   The '237 patent claims are not directed at a mathematical relationship or formula.

The '237 patent claims concrete, specific computer systems and methods for cryptographically

protecting and managing access to secure data in multi-party communications.

92.   '237 patent claims transform data from one form into another that will be

recognizable by the intended recipient but secure against decryption by unintended recipients.

93.   IBM in its computer reference guides ("redbooks"), refers to encryption as

"transform[ing] data that is unprotected.

---

[33] *See also* BACKUPEDGE ENCRYPTION WHITEPAPER, MICROLITE CORPORATION at 2 (2003) (describing the technology of asymmetric keys as "new"); Roger Clarke, MESSAGE TRANSMISSION SECURITY (May 1998), http://www.rogerclarke.com/II/CryptoSecy.html ("Public key cryptography is relatively new and technically complex.").

[34] Deepak Panth, Dhananjay Mehta and Rituparna Shelgaonkar, *A Survey on Security Mechanisms of Leading Cloud Service Providers*, in INTERNATIONAL JOURNAL OF COMPUTER APPLICATIONS 98(1) at 34 (July 2014).

Encryption concepts and terminology

Encryption transforms data that is unprotected, or *plain text*, into encrypted data, or *ciphertext*, by using a *key*. Without knowledge of the encryption key, the ciphertext cannot be converted back to plain text.

Bertrand Dufrasne and Robert Tondini, IBM DS8870 DISK ENCRYPTION 6th Edition at 4 (2015) (From a reference guide published by IBM.)

94.   One or more claims of the '237 patent require a specific configuration of electronic devices, a network configuration, and the use of encryption systems to secure communications from access by an intermediary. These are meaningful limitations that tie the claimed methods and systems to specific machines. For example, the below diagram from the '237 patent illustrates a specific configuration of hardware disclosed in the patent.
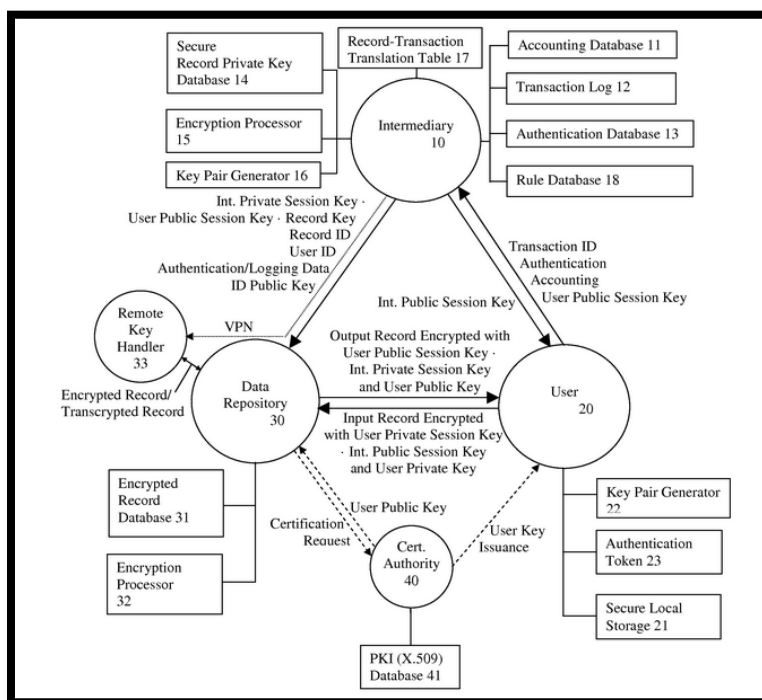
'237 patent, Fig. 1.

2.   U.S. Patent No. 7,181,017

95.   U.S. Patent No. 7,181,017 (the "'017 patent") entitled, System and Method for Secure Three-Party Communications, was filed on March 25, 2002 and claims priority to March 23, 2001. St. Luke is the owner by assignment of the '017 patent. A true and correct copy of the

'017 patent is attached hereto as Exhibit B. The '017 patent claims specific methods and

systems for secure third-party communications—for example, a system and method for

communicating information between a first party and a second party that includes identifying

desired information; negotiating, through an intermediary, a cryptographic comprehension

function for obscuring at least a portion of the information communicated between the first party

and the second party; communicating the encrypted information to the second party, and

decrypting the encrypted information using the negotiated cryptographic comprehension

function. Moreover, in the patented systems and methods, the intermediary does not itself

possess sufficient information to decrypt the encrypted information, thus allowing use of an

"untrusted" intermediary.

96.   The '017 patent has been cited by over 350 issued United States patents as

relevant prior art. Specifically, patents issued to the following companies have cited the '017

patent.

- Electronics and Telecommunications Research Institute (ETRI)
- Sharp Laboratories of America, Inc.
- International Business Machines Corporation
- Microsoft Corporation
- Sony Corporation
- France telecom
- Siemens Medical Solutions USA, Inc.
- Canon Kabushiki Kaisha
- Nikon Corporation
- Apple, Inc.
- Fujitsu Limited
- Hewlett-Packard Development Company, L.P.
- SAP AG
- Guardian Data Storage, Llc
- Teradata US, Inc.
- AT&T Intellectual Property I, L.P.
- Panasonic Corporation
- Sharp Laboratories of America, Inc.
- Ricoh Company, Ltd.
- Nokia Corporation
- Boss Logic, Llc
- Juniper Networks, Inc.
- American Express Travel Related Services Company, Inc.
- Kyocera Mita Corporation
- Oracle International Corporation
- Medox Exchange Inc.
- Nortel Networks Limited

- Hitachi-Omron Terminal Solutions, Corporation
- Medapps, Inc.
- Samsung Electronics Co., Ltd.
- NEC Corporation
- Visa International Service Corporation
- Cisco Technology, Inc.
- Yahoo! Inc.
- Flexera Software Llc
- CompuGroup Medical AG
- Datcard Systems, Inc.
- Futurewei Technologies, Inc.
- Telecome Italia S.P.A.
- General Electric Company
- Fuji Xerox Co., Ltd.
- Massachusetts Institute Of Technology
- Netapp, inc.
- Koninklijke Philips N.V.
- Computer Associates Think, Inc.
- Huawei Technologies Co., Ltd.
- Texas Instruments, Inc.
- Nippon Telegraph And Telephone Corporation
- Research in Motion Limited.
- Net.Orange, Inc.
- Nokia Siemens Networks Oy
- Honeywell Int., Inc.

97.   The claims in the '017 patent are directed at a technical solution to a problem unique to computer networks – securely transmitting encrypted electronic information via an intermediary device, wherein the electronic information is cryptographically secure not only from outside attackers, but also from the intermediary.

98.   At the time of the inventions claimed in the '017 patent, securely processing, transmitting, and accessing protected electronic data in a massively distributed computing environment presented new and unique issues over the state of the art. As explained in the '017 patent: "Often, the nature of these communications protocols places the third party (or group of third parties) in a position of trust, meaning that the third party or parties, without access to additional information, can gain access to private communications or otherwise undermine transactional security or privacy." '017 patent, col. 1:54-61.

> Generating and protecting encryption keys while maintaining data availability has traditionally been a major barrier to implementing encryption, especially on an enterprise scale. Key management is complex and challenging, and often fails because issuance, storage, and renewing are difficult. ***Worse yet, lost keys can make important data permanently unrecoverable***.

Sustainable Compliance for the Payment Card Industry Data Security Standard, ORACLE WHITE PAPER 23 (July 2015) (emphasis added).

99.   Although the systems and methods taught in the '017 patent have been adopted by leading businesses today, at the time of invention, the technologies taught in the '017 patent claims were innovative and novel. "Typical public key encryption technologies, however, presume that a pair of communications partners seek to communicate directly between each other, without the optional or mandatory participation of a third party, and, in fact, are designed specifically to exclude third party monitoring." '017 patent, col. 4:40-45. As described in an article contemporaneous to the '017 patent, the rise of cloud computing and distributed networks gave rise to a need to use key encryption to resolve security issues.

Simon Blake-Wilson, *Information Security, Mathematics and Public-Key Cryptography*, in

stored or communicated. As information becomes increasingly mobile, moving rapidly from application to application and system to system, this feature becomes more and more desirable. Public-key schemes are scalable: their operation is well-suited to environments with lots of users. The advent of large-scale open networks like the Internet necessitates this property.

Designs, Codes and Cryptography, 19, 81 (2000).

100.   Further, the '017 patent claims improve upon the functioning of a computer system by allowing encrypted electronic data to be securely transmitted through an intermediary without the intermediary gaining access to the unencrypted information. This improves the security of the computer system and allows it to be more efficient. [35] "Third parties, however, may offer valuable services to the participants in a communication, but existing protocols for involvement of more than two parties are either inefficient or insecure." '017 patent, col. 4:45-

---

[35] *See* Kevin Hamlen et al., *Security Issues For Cloud Computing* at 39, INTERNATIONAL JOURNAL OF INFORMATION SECURITY AND PRIVACY VOL. 4(2) (April-June 2010) ("The major security challenge with clouds is that the owner of the data may not have control of where the data is placed. . . . Therefore, we need to safeguard the data in the midst of untrusted processes."); Elana Ferrari and Bhavani Thuraisingham, *Security and Privacy for Web Databases and Services* at 17, PROCEEDINGS OF THE EDBT CONFERENCE (March 2003) ("very little work has been devoted to security"); Elisa Bertino et al.; *Selective and Authentic Third-Party Distribution of XML Documents* at 1263, IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, Vol. 16 No. 10 (October 2004) ("The most intuitive solution is that of requiring Publishers to be trusted with regard to the considered security properties. However, this solution could not always be feasible in the Web environment since large Web-based systems cannot be easily verified to be secure.").

48. Studies have confirmed that the inventions disclosed in the '017 patent improve the security of systems.

> ***Key management is a big concern with encryption, because the effectiveness of the solution ultimately depends on protecting the key***. If the key is exposed, the data being protected with the key is, essentially, exposed. Wherever the key is stored, it must be protected, and it should be changed on occasion. For example, if an administrator with access to a key leaves an organization, the key should be changed.

Tanya Baccam, *Transparent Data Encryption: New Technologies and Best Practices for Database Encryption*, SANS WHITE PAPER 3 (April 2010) (emphasis added).

101.   The '017 patent claims are not directed to a "method of organizing human activity," "fundamental economic practice long prevalent in our system of commerce," or "a building block of the modern economy." Instead, they are limited to a concretely circumscribed set of methods and systems for transcrypting electronic information that is transmitted over a computer network via an intermediary.

102.   The '017 patent claims are not directed at the broad concept/idea of "encrypting" or "decrypting" information. Instead, they are limited to a concretely circumscribed set of methods and systems for transcrypting electronic information that is transmitted over a computer network via an intermediary. This type of method and system is unique to the Internet age.

103.   The inventive concepts claimed in the '017 patent are technological, not "entrepreneurial." For example, transcrypting protected electronic information between a first (e.g., server) encrypted form and a second (e.g., network) encrypted form without a substantial intermediate representation of the information in decrypted form is a specific, concrete solution to the technological problem of transferring encrypted information via an intermediary without providing the intermediary substantial access to the information.

104.   Companies such as Oracle have recognized that until recently security for distributed systems was not a primary concern.

Andreas Becker, *High Security for SAP Data with Oracle Database Vault and Transparent Data Encryption*, ORACLE PRESENTATION 6 (2010).

105.   Researchers have identified the problems the '017 patent is directed at solving

arise from new security challenges relating to cloud computing.

Deepak Panth, Dhananjay Mehta and Rituparna Shelgaonkar, *A Survey on Security Mechanisms of Leading Cloud Service Providers*, in INTERNATIONAL JOURNAL OF COMPUTER APPLICATIONS 98(1) at 34 (July 2014) (emphasis added).[36]

106.   The '017 patent claims are directed toward a solution rooted in computer

technology and use technology unique to computers and computer networking to overcome a

problem specifically arising in the realm of secure distributed computing. For example, claims

of the '017 patent require cryptographically manipulating protected electronic information using

one or more intermediary computing devices specially configured to yield a desired result—a

result that overrides the routine and conventional sequence of events in electronic

communications, even encrypted electronic communications.

---

[36] *See also* Vaibhav Khadilkar, Murat Kantarcioglu, and Bhavani Thuraisingham, *Secure Data Processing in a Hybrid Cloud* at 1-2, Computing Research Repository (CoRR) abs/1105.1982 (2011) ("The emergence of cloud computing has created a paradigm shift by allowing parallel processing of massive amounts of data. . . . [H]ow do users protect themselves from cloud service providers who may be able to access their data? This issue is related to data security and is relevant for users since their data is placed at the provider's site.").

107.   The '017 patent is directed to specific problems in the field of cryptography. In the "Background" section of the patent, the '017 patent explains that encryption systems use "keys," similar to passwords, to control how plaintext is encrypted and decrypted. '017 patent, col. 4:39–4:64. An encryption system thereby encrypts and decrypts information differently depending upon the key input. *Id*. Two common cryptanalytic attacks, linear and differential cryptanalysis, analyze large amounts of ciphertext (encrypted information) and different possible keys in order to eventually converge on the correct key and break the encryption. *Id*. Both attacks exploit the fact that some encryption systems use static keys to create the ciphertext. *Id*. In other words, using the same key over and over gives an attacker more information to work with. The inventions of the '017 patent introduce several novel techniques to overcome these weaknesses, particularly where encrypted information is held by an intermediary.

108.   The preemptive effect of the '017 patent is concretely circumscribed by specific limitations. For example, claim 1 of the '017 patent requires:

A method for processing information, comprising the steps of:

receiving information to be processed:

defining a cryptographic comprehension function for the information, adapted for making at least a portion of the information incomprehensible;

receiving asymmetric cryptographic key information, comprising at least asymmetric encryption key information and asymmetric decryption key information;

negotiating a new cryptographic comprehension function between two parties to a communication using an intermediary;

processing the information to invert the cryptographic comprehension function and impose the new cryptographic comprehension function in an integral process, in dependence on at least the asymmetric cryptographic key information, without providing the intermediary with sufficient asymmetric cryptographic key information to decrypt the processed information; and

outputting processed information,

wherein the ability of the asymmetric decryption key information to decrypt the processed information changes dynamically.

109.   The '017 patent does not attempt to preempt every application of the idea of encrypting electronic information transmitted over a computer network, or even the idea of encrypting electronic information transmitted over a computer network via an intermediary.

110.   The '017 patent does not preempt the field of secure third-party communications systems, or prevent use of alternative secure third-party communications systems. For example, the '017 patent includes inventive elements—embodied in specific claim limitations—that concretely circumscribe the patented invention and limit its breadth. These inventive elements are not necessary or obvious tools for achieving secure third-party communications, and they ensure that the claims do not preempt other techniques for secure communications.

111.   For example, the '017 patent describes numerous techniques for secure third-party communications that inform the invention's development but do not, standing alone, fall within the scope of its claims:

- Key Escrow. U.S. Pat. No. 6,009,177 to Sudia, relates to a cryptographic system and method with a key escrow feature that uses a method for verifiably splitting users' private encryption keys into components and for sending those components to trusted agents chosen by the particular users.

- Partitioning of Information Storage Systems. U.S. Patent No. 5,956,400 to Chaum, relates to partitioned information storage systems with controlled retrieval.

- Use of a Trusted Intermediary. U.S. Patent No. 6,161,181 to Haynes, describing secure electronic transactions using a trusted Intermediary; U.S. Patent No. 6,145,079 to Misty, describing secure electronic transactions using a trusted intermediary to perform electronic services.

- Split Key Storage. U.S. Patent No. 6,118,874 to Okamoto, teaching encrypted data using split storage key and system.

- Use of a Cryptographic File Labeling System. U.S. Pat. No. 5,953,419 to Lohstroh, disclosing cryptographic file labeling system for supporting secured access by multiple users.

- Computer Security Devices. U.S. Pat. No. 5,982,520 to Weiser, disclosing a personal storage device for receipt, storage, and transfer of digital information to other electronic

45

devices; *see also* U.S. Pat. No. 5,991,519 to Benhammou; U.S. Pat. No. 5,999,629 to Heer; and U.S. Pat. No. 6,034,618 to Tatebayashi.

- Computer Network Firewalls and Agents. U.S. Pat. No. 6,061,798 to Coley, disclosed the use of an assigned proxy agent to verify the authority of an incoming request to access a network element indicated in the request. Once verified, the proxy agent completes the connection to the protected network element on behalf of the source of the incoming request; *see also* U.S. Pat. No. 6,023,762 to Dean, disclosing a data access and retrieval system which comprises a plurality of user data sources each storing electronic data signals describing data specific to a user, or enabling services selected by a user; an agent device which is configurable to select individual ones of the user data sources and present selections of user data and service data to a set of callers who may interrogate the agent device remotely over a communications network; and U.S. Pat. No. 6,029,150 to Kravitz, disclosing a system and method of payment in an electronic payment system wherein a plurality of customers have accounts with an agent. Further, the patent lists thirty-three other patented systems involving Computer Network Firewalls that are not, standing alone, preempted by the inventions claimed in the patents-in-suit.

- Virtual Private Networks. As described in: U.S. Pat. No. 6,079,020 to Liu and U.S. Pat. No. 6,081,900 and twenty other patented systems involving virtual private networks that are not, standing alone, preempted by the inventions claimed in the patents-in-suit.

- Biometric Authentication. U.S. Pat. No. 5,193,855 to Shamos, disclosing the use of biometrics such as fingerprints to facilitate secure communications and identification of users. Further, the '017 lists numerous patented systems that use biometric authentication that are not, standing alone, preempted by the inventions claimed in the patents-in-suit.

112.   Although "[e]ncryption, in general, represents a basic building block of human ingenuity that has been used for hundreds, if not thousands, of years,"[37] the claims in the '017 patent do not claim, or attempt to preempt, "some process that involves the encryption of data for some purpose" (or similar abstraction).

---

[37] *Paone v. Broadcom Corp.,* Case No. 15 CIV. 0596 BMC GRB, 2015 WL 4988279, at *7 (E.D.N.Y. Aug. 19, 2015) (*citing Fid. Nat'l Info. Servs., Inc.*, Petitioner, CBM2014-00021, 2015 WL 1967328, at *8 (Apr. 29, 2015) (both upholding the patent eligibility of patents directed toward encryption).

113.   The '017 patent does not claim, or attempt to preempt, the performance of an

abstract business practice on the Internet or using a conventional computer

114.   The claimed subject matter of the '017 patent is not a pre-existing but

undiscovered algorithm.

115.   The '017 patent claims systems and methods that "could not conceivably be

performed in the human mind or pencil and paper."[38]

116.   The claims in the '017 patent require the modifying of data that has concrete and

valuable effects in the field of secure third-party communications. By allowing an intermediary

to receive secure information but not gain access to the unencrypted form of the information, the

'017 patent improves the security of computer systems. Prior art systems that the '017 patent

remedies enabled unauthorized "access to private communications or otherwise undermine[d]

transactional security or privacy." Companies have described the use of encryption in the cloud

as important to improve the security and functioning of systems.

> For many organizations, keeping data private and secure has also become a
> compliance requirement. Standards including Health Insurance Portability and
> Accountability Act of 1996 (HIPAA), Sarbanes-Oxley (SOX), Payment Card
> Industry Data Security Standard (PCI DSS), the Gramm-Leach-Bliley Act, and
> EU Data Protection Directives all ***require that organizations protect their data at
> rest and provide defenses against threats***.

HP ATALLA CLOUD ENCRYPTION: SECURING DATA IN THE CLOUD, HP TECHNICAL WHITE PAPER
2 (2014).

117.   The '017 patent claims systems and methods not merely for transferring secure

information over a computer network, but for making the computer network itself more secure.

118.   The claimed invention in the '017 claims is rooted in computer technology and

overcame problems specifically arising in the realm of computer networks.

---

[38] *TQP Dev., LLC v. Intuit Inc.*, Case No. 2:12-CV-180-WCB, 2014 WL 651935, at *4 (E.D.
Tex. Feb. 19, 2014) ((finding claims directed to encryption to be patent eligible); *see also Paone
v. Broadcom Corp.,* Case No. 15 CIV. 0596 BMC GRB, 2015 WL 4988279, at *7 (E.D.N.Y.
Aug. 19, 2015); *see also Prism Technologies, LLC v. T-Mobile USA, Inc.*, 12-cv-124, Dkt. No.
428 at 7 (D. Neb. Sept. 22, 2015) (Finding on cross motions for summary judgment that patents
directed at delivering resources over an untrusted network were patent eligible. "The problems
addressed by Prism's claims are ones that 'arose uniquely in the context of the Internet.'").

119.   The systems and methods claimed in the '017 patent were not a longstanding or fundamental economic practice at the time of patented inventions. Nor were they fundamental principles in ubiquitous use on the Internet or computers in general. As just one example, at the time the inventions disclosed in the '017 patent were conceived, the use of asymmetric encryption keys was described by Oracle as "relatively new."[39]

> A Public Key Infrastructure (PKI) consists of protocols, services, and standards supporting applications of public key cryptography. *Because the technology is still relatively new*, the term PKI is somewhat loosely defined.

INTRODUCTION TO THE SSL TECHNOLOGY, ORACLE DOCUMENTATION (February 1, 2001), http://docs.oracle.com/cd/E53645_01/tuxedo/docs12cr2/security/publickey.html

120.   The asserted claims do not involve a method of doing business implemented on a computer; instead, it involves a method for changing data in a way that will affect the communication system itself, by making it more secure. The security challenges that the '017 patent is directed at were new and unique to distributed networks as confirmed in a recent paper from Accenture Services Pvt. Ltd.: "The unprecedented growth of cloud computing has created new security challenges. The problem is ever more complex as there is a transition from traditional computing to a service-based computing."[40]

121.   The '017 patent claims are not directed to a mathematical relationship or formula. The '017 patent claims concrete, specific computer systems and methods for cryptographically protecting and managing access to secure data in multi-party communications.

122.   The '017 patent claims cover a systems and methods that transform data from one form into another that will be recognizable by the intended recipient but secure against decryption by unintended recipients. IBM, in its reference guides ("redbooks"), refers to encryption as "transform[ing] data that is unprotected."

---

[39] *See also* BACKUPEDGE ENCRYPTION WHITEPAPER, MICROLITE CORPORATION at 2 (2003) (describing the technology of asymmetric keys as "new"); Roger Clarke, MESSAGE TRANSMISSION SECURITY (May 1998), http://www.rogerclarke.com/II/CryptoSecy.html ("Public key cryptography is relatively new and technically complex.").

[40] Deepak Panth, Dhananjay Mehta and Rituparna Shelgaonkar, *A Survey on Security Mechanisms of Leading Cloud Service Providers*, in INTERNATIONAL JOURNAL OF COMPUTER APPLICATIONS 98(1) at 34 (July 2014).

Encryption concepts and terminology

Encryption transforms data that is unprotected, or *plain text*, into encrypted data, or *ciphertext*, by using a *key*. Without knowledge of the encryption key, the ciphertext cannot be converted back to plain text.

Bertrand Dufrasne and Robert Tondini, IBM DS8870 DISK ENCRYPTION 6th Edition at 4 (2015) (From a reference guide published by IBM.)

123.   One or more claims of the '017 patent require a specific configuration of electronic devices, a network configuration, and the use of encryption systems to secure communications from access by an intermediary. These are meaningful limitations that tie the claimed methods and systems to specific machines. For example, the below diagram from the '017 patent illustrates a specific configuration of hardware disclosed in the patent.
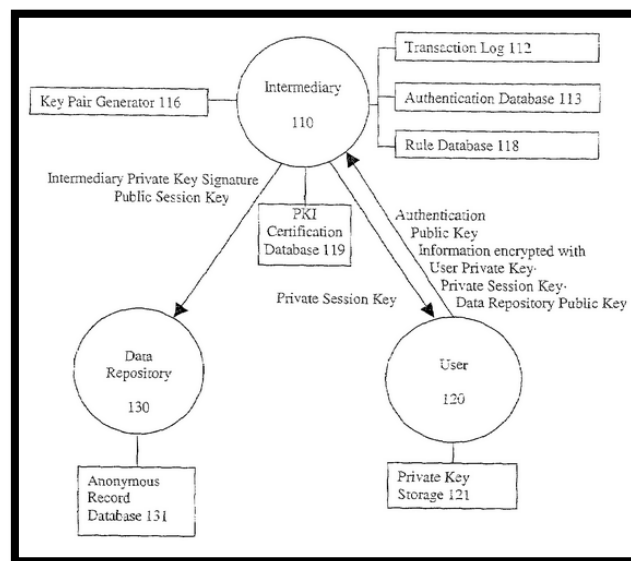
'017 patent, Fig. 2.

3.   U.S. Patent No. 7,869,591

124.   U.S. Patent No. 7,869,591 (the "'591 patent") entitled, System and Method for Secure Three-Party Communications, was filed on February 16, 2007, and claims priority to March 23, 2001. St. Luke is the owner by assignment of the '591 patent. A true and correct copy of the '591 patent is attached hereto as Exhibit C.

125.   The '591 patent has been cited by over twenty issued United States patents as relevant prior art. Specifically, patents issued to the following companies have cited the '591 patent.

- Square, Inc.
- Konnklike Philips Electronics, N.V
- Red Hat, Inc.
- Microsoft Corporation
- Industrial Technology Research Institute ("ITRI")
- Electronics and Telecommunications Research Institute (ETRI)
- Saas Document Solutions Limited
- Good Technology Corporation
- Avanade Inc.
- Medical Management International, Inc.

126.   The '591 patent claims specific methods and systems for secure third-party communications—for example, a system and method for communicating information between a first party and a second party that includes identifying desired information; negotiating, through an intermediary, a cryptographic comprehension function for obscuring at least a portion of the information communicated between the first party and the second party; communicating the encrypted information to the second party; and decrypting the encrypted information using the negotiated cryptographic comprehension function. Moreover, in the patented systems and methods, the intermediary does not itself possess sufficient information to decrypt the encrypted information, thus allowing use of an "untrusted" intermediary.

127.   The claims in the '591 patent are directed at a technical solution to a problem unique to computer networks – securely transmitting encrypted electronic information via an intermediary device, wherein the electronic information is cryptographically secure not only from outside attackers, but also from the intermediary.

128.   At the time of the inventions claimed in the '591 patent, securely processing, transmitting, and accessing protected electronic data in a massively distributed computing environment presented new and unique issues over the state of the art. As explained in the '591 patent: "Often, the nature of these communications protocols places the third party (or group of third parties) in a position of trust, meaning that the third party or parties, without access to

additional information, can gain access to private communications or otherwise undermine

transactional security or privacy." '591 patent, col. 2:10-15.

> Generating and protecting encryption keys while maintaining data availability has traditionally been a major barrier to implementing encryption, especially on an enterprise scale. Key management is complex and challenging, and often fails because issuance, storage, and renewing are difficult. ***Worse yet, lost keys can make important data permanently unrecoverable***.

Sustainable Compliance for the Payment Card Industry Data Security Standard, ORACLE WHITE PAPER 23 (July 2015) (emphasis added).

129.   Although the systems and methods taught in the '591 patent have been adopted by

leading businesses today, at the time of invention, the technologies taught in the '591 patent

claims were innovative and novel. "Typical public key encryption technologies, however,

presume that a pair of communications partners seek to communicate directly between each

other, without the optional or mandatory participation of a third party, and, in fact, are designed

specifically to exclude third party monitoring." '591 patent, col. 2:54-69. As described in an

article contemporaneous to the '591 patent, the rise of cloud computing and distributed networks

gave rise to a need to use key encryption to resolve security issues.

> stored or communicated. As information becomes increasingly mobile, moving rapidly from application to application and system to system, this feature becomes more and more desirable. Public-key schemes are scalable: their operation is well-suited to environments with lots of users. The advent of large-scale open networks like the Internet necessitates this property.

Simon Blake-Wilson, *Information Security, Mathematics and Public-Key Cryptography*, in Designs, Codes and Cryptography, 19, 81 (2000).

130.   Further, the '591 patent claims improve upon the functioning of a computer

system by allowing encrypted electronic data to be securely transmitted through an intermediary

without the intermediary gaining access to the unencrypted information. This improves the

security of the computer system and allows it to be more efficient. [41] "Third parties, however,

---

[41] *See* Kevin Hamlen et al., *Security Issues For Cloud Computing* at 39, INTERNATIONAL JOURNAL OF INFORMATION SECURITY AND PRIVACY VOL. 4(2) (April-June 2010) ("The major security challenge with clouds is that the owner of the data may not have control of where the data is placed. . . . Therefore, we need to safeguard the data in the midst of untrusted processes."); Elana Ferrari and Bhavani Thuraisingham, *Security and Privacy for Web*

may offer valuable services to the participants in a communication, but existing protocols for

involvement of more than two parties are either inefficient or insecure." '591 patent, col. 2:59-

62. Studies have confirmed that the inventions disclosed in the '591 patent improve the security

of systems.

> ***Key management is a big concern with encryption, because the effectiveness of
> the solution ultimately depends on protecting the key***. If the key is exposed, the
> data being protected with the key is, essentially, exposed. Wherever the key is
> stored, it must be protected, and it should be changed on occasion. For example,
> if an administrator with access to a key leaves an organization, the key should be
> changed.

Tanya Baccam, *Transparent Data Encryption: New Technologies and Best Practices for
Database Encryption*, SANS WHITE PAPER 3 (April 2010) (emphasis added).

131.   The '591 patent claims are not directed to a "method of organizing human

activity," "fundamental economic practice long prevalent in our system of commerce," or "a

building block of the modern economy." Instead, they are limited to a concretely circumscribed

set of methods and systems for transcrypting electronic information that is transmitted over a

computer network via an intermediary.

132.   The '591 patent claims are not directed at the broad concept/idea of "encrypting"

or "decrypting" information. Instead, they are limited to a concretely circumscribed set of

methods and systems for transcrypting electronic information that is transmitted over a computer

network via an intermediary. This type of method and system is unique to the Internet age.

133.   The inventive concepts claimed in the '591 patent are technological, not

"entrepreneurial." For example, transcrypting protected electronic information between a first

(e.g., server) encrypted form and a second (e.g., network) encrypted form without a substantial

intermediate representation of the information in decrypted form is a specific, concrete solution

---

Databases and Services at 17, PROCEEDINGS OF THE EDBT CONFERENCE (March 2003) ("very
little work has been devoted to security"); Elisa Bertino et al.; *Selective and Authentic Third-
Party Distribution of XML Documents* at 1263, IEEE TRANSACTIONS ON KNOWLEDGE AND
DATA ENGINEERING, Vol. 16 No. 10 (October 2004) ("The most intuitive solution is that of
requiring Publishers to be trusted with regard to the considered security properties. However,
this solution could not always be feasible in the Web environment since large Web-based
systems cannot be easily verified to be secure.").

to the technological problem of transferring encrypted information via an intermediary without

providing the intermediary substantial access to the information.

134.   Companies such as Oracle have recognized that until recently security for

distributed systems was not a primary concern.

Andreas Becker, *High Security for SAP Data with Oracle Database Vault and Transparent Data Encryption*, ORACLE PRESENTATION 6 (2010).

135.   Researchers have identified the problems the '591 patent is directed at solving

arise from new security challenges relating to cloud computing.

Deepak Panth, Dhananjay Mehta and Rituparna Shelgaonkar, *A Survey on Security Mechanisms of Leading Cloud Service Providers*, in INTERNATIONAL JOURNAL OF COMPUTER APPLICATIONS 98(1) at 34 (July 2014) (emphasis added). [42]

136.   The '591 patent claims are directed toward a solution rooted in computer

technology and use technology unique to computers and computer networking to overcome a

---

[42] *See also* Vaibhav Khadilkar, Murat Kantarcioglu, and Bhavani Thuraisingham, *Secure Data Processing in a Hybrid Cloud* at 1-2, Computing Research Repository (CoRR) abs/1105.1982 (2011) ("The emergence of cloud computing has created a paradigm shift by allowing parallel processing of massive amounts of data. . . . [H]ow do users protect themselves from cloud service providers who may be able to access their data? This issue is related to data security and is relevant for users since their data is placed at the provider's site.").

problem specifically arising in the realm of secure distributed computing. For example, the claims of the '591 patent require cryptographically manipulating protected electronic information using one or more intermediary computing devices specially configured to yield a desired result—a result that overrides the routine and conventional sequence of events in electronic communications, even encrypted electronic communications.

137. The '591 patent is directed to specific problems in the field of cryptography. In the "Background" section of the patent, the '591 patent explains that encryption systems use "keys," similar to passwords, to control how plaintext is encrypted and decrypted. '591 patent, col. 2:16-37. An encryption system thereby encrypts and decrypts information differently depending upon the key input. *Id*. Two common cryptanalytic attacks, linear and differential cryptanalysis, analyze large amounts of ciphertext (encrypted information) and different possible keys in order to eventually converge on the correct key and break the encryption. *Id*. Both attacks exploit the fact that some encryption systems use static keys to create the ciphertext. *Id*. In other words, using the same key over and over gives an attacker more information to work with. The inventions of the '591 patent introduce several novel techniques to overcome these weaknesses particularly where encrypted information is held by an intermediary.

138. The preemptive effect of the '591 patent is concretely circumscribed by specific limitations. For example, claim 13 of the '591 patent requires:

A method for transcrypting information, comprising:

(a) receiving and storing in a first memory information encrypted based on a first set of cryptographic keys, a first portion of the first set of cryptographic keys having been employed to produce the encrypted information and a second portion of the first set of cryptographic keys being required to decrypt the information encrypted with the first portion of the first set of cryptographic information;

(b) receiving and storing in a second memory a first portion of a second set of cryptographic keys, having a corresponding second portion of the second set of cryptographic keys being required for decryption of a message encrypted using the first portion of the second set of cryptographic keys;

(c) negotiating a set of session keys through a communication port,

(d) generating a transcription key for transforming the received encrypted information to transcrypted information, in dependence on at least:

> (i) information representing the second portion of the first set of cryptographic keys,

> (ii) information representing the first portion of the second set of cryptographic keys; and

> (iii) a first portion of the set of session keys, and

(e) transcrypting the stored encrypted information into transcrypted information using the transcryptiopn key, wherein the generating a transcription key step and the transcrypting the encrypted information step are performed without either requiring or employing sufficient information either to decrypt the encrypted information or to comprehend the transcrypted information.

139.   The '591 patent does not attempt to preempt every application of the idea of encrypting electronic information transmitted over a computer network, or even the idea of encrypting electronic information transmitted over a computer network via an intermediary.

140.   The '591 patent does not preempt the field of secure third-party communications systems, or prevent use of alternative secure third-party communications systems. For example, the '591 patent includes inventive elements—embodied in specific claim limitations—that concretely circumscribe the patented invention and limit its breadth. These inventive elements are not necessary or obvious tools for achieving secure third-party communications, and they ensure that the claims do not preempt other techniques for secure communications.

141.   For example, the '591 patent describes numerous techniques for secure third-party communications that inform the invention's development but do not, standing alone, fall within the scope of its claims:

- Key Escrow. U.S. Pat. No. 6,009,177 to Sudia, relates to a cryptographic system and method with a key escrow feature that uses a method for verifiably splitting users' private encryption keys into components and for sending those components to trusted agents chosen by the particular users.

- Partitioning of Information Storage Systems. U.S. Patent No. 5,956,400 to Chaum, relates to partitioned information storage systems with controlled retrieval.

- Use of a Trusted Intermediary. U.S. Patent No. 6,161,181 to Haynes, describing secure electronic transactions using a trusted Intermediary; U.S. Patent No. 6,145,079 to Misty, describing secure electronic transactions using a trusted intermediary to perform electronic services.

- Split Key Storage. U.S. Patent No. 6,118,874 to Okamoto, teaching encrypted data using split storage key and system.

- Use of a Cryptographic File Labeling System. U.S. Pat. No. 5,953,419 to Lohstroh, disclosing cryptographic file labeling system for supporting secured access by multiple users.

- Computer Security Devices. U.S. Pat. No. 5,982,520 to Weiser, disclosing a personal storage device for receipt, storage, and transfer of digital information to other electronic devices; *see also* U.S. Pat. No. 5,991,519 to Benhammou; U.S. Pat. No. 5,999,629 to Heer; and U.S. Pat. No. 6,034,618 to Tatebayashi.

- Computer Network Firewalls And Agents. U.S. Pat. No. 6,061,798 to Coley, disclosed the use of an assigned proxy agent to verify the authority of an incoming request to access a network element indicated in the request. Once verified, the proxy agent completes the connection to the protected network element on behalf of the source of the incoming request; *see also* U.S. Pat. No. 6,023,762 to Dean, disclosing a data access and retrieval system which comprises a plurality of user data sources each storing electronic data signals describing data specific to a user, or enabling services selected by a user; an agent device which is configurable to select individual ones of the user data sources and present selections of user data and service data to a set of callers who may interrogate the agent device remotely over a communications network; and U.S. Pat. No. 6,029,150 to Kravitz, disclosing a system and method of payment in an electronic payment system wherein a plurality of customers have accounts with an agent. Further, the patent lists thirty-three other patented systems involving Computer Network Firewalls that are not, standing alone, preempted by the inventions claimed in the patents-in-suit.

- Virtual Private Networks. As described in: U.S. Pat. No. 6,079,020 to Liu and U.S. Pat. No. 6,081,900 and twenty other patented systems involving virtual private networks that are not, standing alone, preempted by the inventions claimed in the patents-in-suit.

- Biometric Authentication. U.S. Pat. No. 5,193,855 to Shamos, disclosing the use of biometrics such as fingerprints to facilitate secure communications and identification of users. Further, the '591 lists numerous patented systems that use biometric

authentication that are not, standing alone, preempted by the inventions claimed in the patents-in-suit.

142.   Although "[e]ncryption, in general, represents a basic building block of human ingenuity that has been used for hundreds, if not thousands, of years,"[43] the claims in the '591 patent do not claim, or attempt to preempt, "some process that involves the encryption of data for some purpose" (or similar abstraction).

143.   The '591 patent does not claim, or attempt to preempt, the performance of an abstract business practice on the Internet or using a conventional computer

144.   The claimed subject matter of the '591 patent is not a pre-existing but undiscovered algorithm.

145.   The '591 patent claims systems and methods that "could not conceivably be performed in the human mind or pencil and paper."[44]

146.   The claims in the '591 patent require the modifying of data that has concrete and valuable effects in the field of secure third-party communications. By allowing an intermediary to receive secure information but not gain access to the unencrypted form of the information, the '591 patent improves the security of computer systems. Prior art systems that the '591 patent remedies enabled unauthorized "access to private communications or otherwise undermine[d] transactional security or privacy." Companies have described the use of encryption in the cloud as important to improve the security and functioning of systems.

> For many organizations, keeping data private and secure has also become a compliance requirement. Standards including Health Insurance Portability and

---

[43] *Paone v. Broadcom Corp.,* Case No. 15 CIV. 0596 BMC GRB, 2015 WL 4988279, at *7 (E.D.N.Y. Aug. 19, 2015) (*citing Fid. Nat'l Info. Servs., Inc.*, Petitioner, CBM2014-00021, 2015 WL 1967328, at *8 (Apr. 29, 2015) (both upholding the patent eligibility of patents directed toward encryption).

[44] *TQP Dev., LLC v. Intuit Inc.*, Case No. 2:12-CV-180-WCB, 2014 WL 651935, at *4 (E.D. Tex. Feb. 19, 2014) ((finding claims directed to encryption to be patent eligible); *see also Paone v. Broadcom Corp.,* Case No. 15 CIV. 0596 BMC GRB, 2015 WL 4988279, at *7 (E.D.N.Y. Aug. 19, 2015); *see also Prism Technologies, LLC v. T-Mobile USA, Inc.*, 12-cv-124, Dkt. No. 428 at 7 (D. Neb. Sept. 22, 2015) (Finding on cross motions for summary judgment that patents directed at delivering resources over an untrusted network were patent eligible. "The problems addressed by Prism's claims are ones that 'arose uniquely in the context of the Internet.'").

Accountability Act of 1996 (HIPAA), Sarbanes-Oxley (SOX), Payment Card Industry Data Security Standard (PCI DSS), the Gramm-Leach-Bliley Act, and EU Data Protection Directives all *require that organizations protect their data at rest and provide defenses against threats*.

HP ATALLA CLOUD ENCRYPTION: SECURING DATA IN THE CLOUD, HP TECHNICAL WHITE PAPER 2 (2014).

147.   The '591 patent claims systems and methods not merely for transferring secure information over a computer network, but for making the computer network itself more secure.

148.   The claimed invention in the '591 claims is rooted in computer technology and overcame problems specifically arising in the realm of computer networks.

149.   The systems and methods claimed in the '591 patent were not a longstanding or fundamental economic practice at the time of patented inventions. Nor were they fundamental principles in ubiquitous use on the Internet or computers in general. As just one example, at the time the inventions disclosed in the '591 patent were conceived, the use of asymmetric encryption keys was described by Oracle as "relatively new."[45]

A Public Key Infrastructure (PKI) consists of protocols, services, and standards supporting applications of public key cryptography. *Because the technology is still relatively new*, the term PKI is somewhat loosely defined.

INTRODUCTION TO THE SSL TECHNOLOGY, ORACLE DOCUMENTATION (February 1, 2001), http://docs.oracle.com/cd/E53645_01/tuxedo/docs12cr2/security/publickey.html
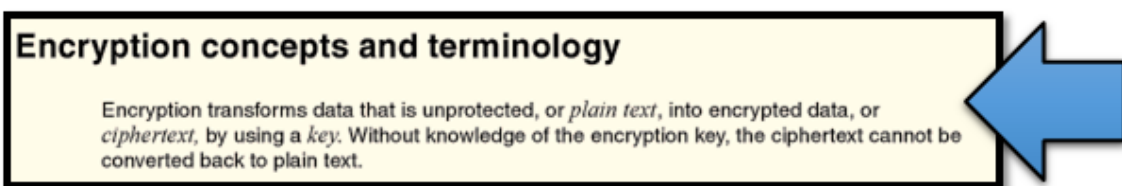
150.   The asserted claims do not involve a method of doing business that happens to be implemented on a computer; instead, it involves a method for changing data in a way that will affect the communication system itself, by making it more secure. The security challenges that the '591 patent is directed at were new and unique to distributed networks as confirmed in a recent paper from Accenture Services Pvt. Ltd.: "The unprecedented growth of cloud computing has created new security challenges. The problem is ever more complex as there is a transition from traditional computing to a service-based computing."[46]

---

[45] *See also* BACKUPEDGE ENCRYPTION WHITEPAPER, MICROLITE CORPORATION at 2 (2003) (describing the technology of asymmetric keys as "new"); Roger Clarke, MESSAGE TRANSMISSION SECURITY (May 1998), http://www.rogerclarke.com/II/CryptoSecy.html ("Public key cryptography is relatively new and technically complex.").

[46] Deepak Panth, Dhananjay Mehta and Rituparna Shelgaonkar, *A Survey on Security Mechanisms of Leading Cloud Service Providers*, in INTERNATIONAL JOURNAL OF COMPUTER APPLICATIONS 98(1) at 34 (July 2014).

151.   The '591 patent claims are not directed at a mathematical relationship or formula. The '591 patent claims concrete, specific computer systems and methods for cryptographically protecting and managing access to secure data in multi-party communications.

152.   '591 patent claims transform data from one form into another that will be recognizable by the intended recipient but secure against decryption by unintended recipients. IBM, in its reference guides ("redbooks"), refers to encryption as "transform[ing] data that is unprotected.

Encryption concepts and terminology

Encryption transforms data that is unprotected, or *plain text*, into encrypted data, or *ciphertext*, by using a *key*. Without knowledge of the encryption key, the ciphertext cannot be converted back to plain text.

Bertrand Dufrasne and Robert Tondini, IBM DS8870 DISK ENCRYPTION 6th Edition at 4 (2015) (From a reference guide published by IBM.)

153.   One or more claims of the '591 patent require a specific configuration of electronic devices, a network configuration, and the use of encryption systems to secure communications from access by an intermediary. These are meaningful limitations that tie the claimed methods and systems to specific machines. For example, the below diagram from the '591 patent illustrates a specific configuration of hardware disclosed in the patent.
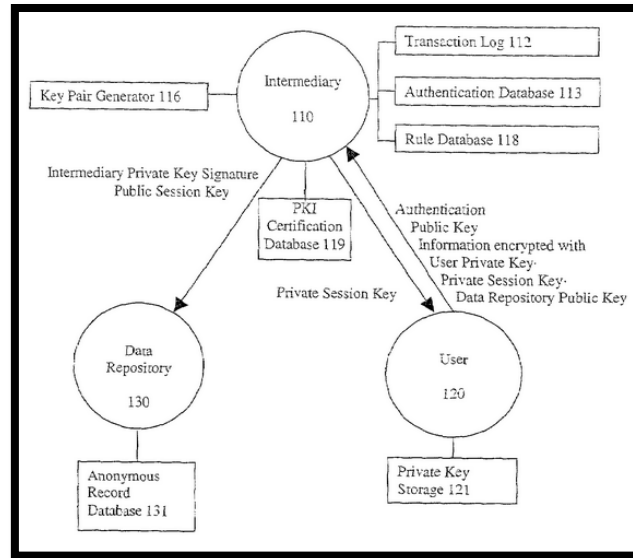
'591 patent, Fig. 2.

4. **U.S. Patent No. 8,904,181**

154.   U.S. Patent No. 8,904,181 (the "'181 patent") entitled, System and Method for Secure Three-Party Communications, was filed on November 20, 2012 and claims priority to March 23, 2001. St. Luke is the owner by assignment of the '181 patent. A true and correct copy of the '181 patent is attached hereto as Exhibit D. The '181 patent claims specific methods and systems for securely transcrypting protected electronic information transmitted over at least one computer network from a first encrypted form to a second, different encrypted form substantially without intermediate decryption of the protected electronic information.

155.   The '181 patent claims a technical solution to a problem unique to computer networks – securely transmitting encrypted electronic information via an intermediary device, wherein the electronic information is cryptographically secure not only from outside attackers, but also from the intermediary.

156.   At the time of the inventions claimed in the '181 patent, securely processing, transmitting, and accessing protected electronic data in a massively distributed computing environment presented new and unique issues over the state of the art. As explained in the '181 patent: "Often, the nature of these communications protocols places the third party (or group of third parties) in a position of trust, meaning that the third party or parties, without access to

60

additional information, can gain access to private communications or otherwise undermine transactional security or privacy." '181 patent, col. 2:14-20.

> Generating and protecting encryption keys while maintaining data availability has traditionally been a major barrier to implementing encryption, especially on an enterprise scale. Key management is complex and challenging, and often fails because issuance, storage, and renewing are difficult. ***Worse yet, lost keys can make important data permanently unrecoverable***.

Sustainable Compliance for the Payment Card Industry Data Security Standard, ORACLE WHITE PAPER 23 (July 2015) (emphasis added).

157.   Although the systems and methods taught in the '181 patent have been adopted by leading businesses today, at the time of invention, the technologies taught in the '181 patent claims were innovative and novel. "Typical public key encryption technologies, however, presume that a pair of communications partners seek to communicate directly between each other, without the optional or mandatory participation of a third party, and, in fact, are designed specifically to exclude third party monitoring." '181 patent, col. 2:59-64. Indeed, companies such as Oracle have recognized that, until recently, security for distributed systems was not a primary concern.

Andreas Becker, *High Security for SAP Data with Oracle Database Vault and Transparent Data Encryption*, ORACLE PRESENTATION 6 (2010).

158.   Further, the '181 patent claims improve upon the functioning of a computer system by allowing encrypted electronic data to be securely transmitted through an intermediary without the intermediary gaining substantial access to the unencrypted information. This improves the security of the computer system and allows it to be more efficient. [47] "Third

---

[47] *See* Kevin Hamlen et al., *Security Issues For Cloud Computing* at 39, INTERNATIONAL JOURNAL OF INFORMATION SECURITY AND PRIVACY VOL. 4(2) (April-June 2010) ("The major security challenge with clouds is that the owner of the data may not have control of where the

parties, however, may offer valuable services to the participants in a communication, but existing protocols for involvement of more than two parties are either inefficient or insecure." '181 patent, col. 2:64-67. Studies have confirmed that the inventions disclosed in the '181 patent improve the security of systems.

> ***Key management is a big concern with encryption, because the effectiveness of the solution ultimately depends on protecting the key***. If the key is exposed, the data being protected with the key is, essentially, exposed. Wherever the key is stored, it must be protected, and it should be changed on occasion. For example, if an administrator with access to a key leaves an organization, the key should be changed.

Tanya Baccam, *Transparent Data Encryption: New Technologies and Best Practices for Database Encryption*, SANS WHITE PAPER 3 (April 2010) (emphasis added).

159.   The '181 patent claims are not directed to a "method of organizing human activity," "fundamental economic practice long prevalent in our system of commerce," or "a building block of the modern economy." Instead, they are limited to a concretely circumscribed set of methods and systems for transcrypting electronic information that is transmitted over a computer network via an intermediary.

160.   The '181 patent claims are not directed at the broad concept/idea of "encrypting" or "decrypting" information. Instead, they are limited to a concretely circumscribed set of methods and systems for transcrypting electronic information that is transmitted over a computer network via an intermediary. These methods and systems are technologies unique to the Internet age.

161.   The inventive concepts claimed in the '181 patent are technological, not "entrepreneurial." For example, transcrypting protected electronic information between a first

---

data is placed. . . . Therefore, we need to safeguard the data in the midst of untrusted processes."); Elana Ferrari and Bhavani Thuraisingham, *Security and Privacy for Web Databases and Services* at 17, PROCEEDINGS OF THE EDBT CONFERENCE (March 2003) ("very little work has been devoted to security"); Elisa Bertino et al.; *Selective and Authentic Third-Party Distribution of XML Documents* at 1263, IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, Vol. 16 No. 10 (October 2004) ("The most intuitive solution is that of requiring Publishers to be trusted with regard to the considered security properties. However, this solution could not always be feasible in the Web environment since large Web-based systems cannot be easily verified to be secure.").

(e.g., server) encrypted form and a second (e.g., network) encrypted form without a substantial intermediate representation of the information in decrypted form is a specific, concrete solution to the technological problem of transferring encrypted information via an intermediary without providing the intermediary substantial access to the information.

162.   Researchers have identified the problems the '181 patent is directed at solving arise from new security challenges relating to cloud computing.

Deepak Panth, Dhananjay Mehta and Rituparna Shelgaonkar, *A Survey on Security Mechanisms of Leading Cloud Service Providers*, in INTERNATIONAL JOURNAL OF COMPUTER APPLICATIONS 98(1) at 34 (July 2014) (emphasis added). [48]

163.   The '181 patent claims are directed toward a solution rooted in computer technology and use technology unique to computers and computer networking to overcome a problem specifically arising in the realm of secure distributed computing. For example, claims of the '181 patent require transcrypting protected electronic information using one or more intermediary computing devices specially configured to yield a desired result—a result that overrides the routine and conventional sequence of events in electronic communications, even encrypted electronic communications.

164.   The '181 patent is directed to specific problems in the field of cryptography. In the "Background" section of the patent, the '181 patent explains that encryption systems use "keys," similar to passwords, to control how plaintext is encrypted and decrypted. '181 patent,

---

[48] *See also* Vaibhav Khadilkar, Murat Kantarcioglu, and Bhavani Thuraisingham, *Secure Data Processing in a Hybrid Cloud* at 1-2, Computing Research Repository (CoRR) abs/1105.1982 (2011) ("The emergence of cloud computing has created a paradigm shift by allowing parallel processing of massive amounts of data. . . . [H]ow do users protect themselves from cloud service providers who may be able to access their data? This issue is related to data security and is relevant for users since their data is placed at the provider's site.").

col. 2:11–5:8. An encryption system thereby encrypts and decrypts information differently depending upon the key input. *Id*. Two common cryptanalytic attacks, linear and differential cryptanalysis, analyze large amounts of ciphertext (encrypted information) and different possible keys in order to eventually converge on the correct key and break the encryption. *Id*. at col. 4:10–4:27.

165. Both attacks exploit the fact that some encryption systems use static keys to create the ciphertext. *Id*. In other words, using the same key over and over gives an attacker more information to work with. The inventions of the '181 patent introduce several novel techniques to overcome these weaknesses and allow encrypted information to be securely transferred through an intermediary.

166. The preemptive effect of the claims of the '181 patent are concretely circumscribed by specific limitations. For example, claim 1 of the '181 patent requires:

> A key handler, comprising:
>
> > an interface to a memory which stores a plurality of encrypted records, each encrypted record having an associated asymmetric encryption key pair and being encrypted with a first component of the associated asymmetric encryption key pair;
> >
> > at least one automated processor operating in a privileged processing environment, configured to receive a selected encrypted record from the memory through the interface, to negotiate at least one asymmetric session key, and to transcrypt the encrypted message to a transcrypted message in an integral process substantially without intermediate decryption, using a transcryption key derived at least in part from the at least one asymmetric session key; and
> >
> > a communication port configured to conduct the negotiation for the at least one asymmetric session key and to communicate the transcrypted record.

167. The '181 patent does not attempt to preempt every application of the idea of encrypting electronic information transmitted over a computer network, or even the idea of encrypting electronic information transmitted over a computer network via an intermediary.

168.   The '181 patent does not preempt the field of secure third-party communications systems, or prevent use of alternative secure third-party communications systems. For example, the '181 patent includes inventive elements—embodied in specific claim limitations—that concretely circumscribe the patented invention and greatly limit its breadth. These inventive elements are not necessary or obvious tools for achieving secure third-party communications, and they ensure that the claims do not preempt other techniques for secure communications.

169.   For example, the '181 patent describes numerous techniques for secure third-party communications that inform the invention's development but do not, standing alone, fall within the scope of its claims:

- Key Escrow. U.S. Pat. No. 6,009,177 to Sudia, relates to a cryptographic system and method with a key escrow feature that uses a method for verifiably splitting users' private encryption keys into components and for sending those components to trusted agents chosen by the particular users.

- Partitioning of Information Storage Systems. U.S. Patent No. 5,956,400 to Chaum, relates to partitioned information storage systems with controlled retrieval.

- Use of a Trusted Intermediary. U.S. Patent No. 6,161,181 to Haynes, describing secure electronic transactions using a trusted Intermediary; U.S. Patent No. 6,145,079 to Misty, describing secure electronic transactions using a trusted intermediary to perform electronic services.

- Split Key Storage. U.S. Patent No. 6,118,874 to Okamoto, teaching encrypted data using split storage key and system.

- Use of a Cryptographic File Labeling System. U.S. Pat. No. 5,953,419 to Lohstroh, disclosing cryptographic file labeling system for supporting secured access by multiple users.

- Computer Security Devices. U.S. Pat. No. 5,982,520 to Weiser, disclosing a personal storage device for receipt, storage, and transfer of digital information to other electronic devices; *see also* U.S. Pat. No. 5,991,519 to Benhammou; U.S. Pat. No. 5,999,629 to Heer; and U.S. Pat. No. 6,034,618 to Tatebayashi.

- Computer Network Firewalls and Agents. U.S. Pat. No. 6,061,798 to Coley, disclosed the use of an assigned proxy agent to verify the authority of an incoming request to

access a network element indicated in the request. Once verified, the proxy agent completes the connection to the protected network element on behalf of the source of the incoming request; *see also* U.S. Pat. No. 6,023,762 to Dean, disclosing a data access and retrieval system which comprises a plurality of user data sources each storing electronic data signals describing data specific to a user, or enabling services selected by a user; an agent device which is configurable to select individual ones of the user data sources and present selections of user data and service data to a set of callers who may interrogate the agent device remotely over a communications network; and U.S. Pat. No. 6,029,150 to Kravitz, disclosing a system and method of payment in an electronic payment system wherein a plurality of customers have accounts with an agent. Further, the patent lists thirty-three other patented systems involving Computer Network Firewalls that are not, standing alone, preempted by the inventions claimed in the patents-in-suit.

- Virtual Private Networks. As described in: U.S. Pat. No. 6,079,020 to Liu and U.S. Pat. No. 6,081,900 and twenty other patented systems involving virtual private networks that are not, standing alone, preempted by the inventions claimed in the patents-in-suit.

- Biometric Authentication. U.S. Pat. No. 5,193,855 to Shamos, disclosing the use of biometrics such as fingerprints to facilitate secure communications and identification of users. Further, the '181 patent lists hundreds of patented systems that use biometric authentication that are not, standing alone, preempted by the inventions claimed in the patents-in-suit.

170.   Although "[e]ncryption, in general, represents a basic building block of human ingenuity that has been used for hundreds, if not thousands, of years,"[49] the '181 patent does not claim, or attempt to preempt, "some process that involves the encryption of data for some purpose" (or similar abstraction).

171.   The '181 patent does not claim, or attempt to preempt, the performance of an abstract business practice on the Internet or using a conventional computer.

172.   The claimed subject matter of the '181 patent is not a pre-existing but undiscovered algorithm.

---

[49] *Paone v. Broadcom Corp.,* Case No. 15 CIV. 0596 BMC GRB, 2015 WL 4988279, at *7 (E.D.N.Y. Aug. 19, 2015) (*citing* Fid. Nat'l Info. Servs., Inc., Petitioner, CBM2014-00021, 2015 WL 1967328, at *8 (Apr. 29, 2015) (both upholding the patent eligibility of patents directed toward encryption).

173.   The '181 patent claims systems and methods that "could not conceivably be performed in the human mind or pencil and paper."[50]

174.   The '181 patent claims require the use of a computer system.

175.   The claims in the '181 patent require the modifying of data that has concrete and valuable effects in the field of secure third-party communications. By allowing an intermediary to receive secure information but not gain access to the unencrypted form of the information, the '181 patent improves the security of computer systems. Prior art systems that the '181 patent remedies enabled unauthorized "access to private communications or otherwise undermine[d] transactional security or privacy." Companies have described the use of encryption in the cloud as important to improve the security and functioning of systems.

> For many organizations, keeping data private and secure has also become a compliance requirement. Standards including Health Insurance Portability and Accountability Act of 1996 (HIPAA), Sarbanes-Oxley (SOX), Payment Card Industry Data Security Standard (PCI DSS), the Gramm-Leach-Bliley Act, and EU Data Protection Directives all *require that organizations protect their data at rest and provide defenses against threats*.

HP ATALLA CLOUD ENCRYPTION: SECURING DATA IN THE CLOUD, HP TECHNICAL WHITE PAPER 2 (2014).

176.   The '181 patent claims systems and methods not merely for transferring secure information over a computer network, but for making the computer network itself more secure. [51]

---

[50] *TQP Dev., LLC v. Intuit Inc.*, Case No. 2:12-CV-180-WCB, 2014 WL 651935, at *4 (E.D. Tex. Feb. 19, 2014) (finding claims directed to encryption to be patent eligible); *see also Paone v. Broadcom Corp.,* Case No. 15 CIV. 0596 BMC GRB, 2015 WL 4988279, at *7 (E.D.N.Y. Aug. 19, 2015); *see also Prism Technologies, LLC v. T-Mobile USA, Inc.*, 12-cv-124, Dkt. No. 428 at 7 (D. Neb. Sept. 22, 2015) (Finding on cross motions for summary judgment that patents directed at delivering resources over an untrusted network were patent eligible. "The problems addressed by Prism's claims are ones that 'arose uniquely in the context of the Internet.'").

[51] Limitations in the prior art that the '181 patent was directed to solving included: computer systems where a "third party plays a requisite role in the transaction but which need not be trusted with access to the information or the cryptographic key" (*Id.*, col. 2:6-9); "[p]asswords may be written near access terminals (*Id.* col. 1:52-54);" "[s]ecurity tokens can be stolen or misplaced" (*Id.*, col. 1:54-55); and "users may share supposedly secret information" (*Id.*, col. 1:55).

177.   The claimed invention in the '181 claims is rooted in computer technology and overcomes problems specifically arising in the realm of computer networks.

178.   The systems and methods claimed in the '181 patent were not a longstanding or fundamental economic practice at the time of patented inventions. Nor were they fundamental principles in ubiquitous use on the Internet or computers in general. As just one example, at the time the inventions disclosed in the '181 patent were conceived, the use of asymmetric encryption keys was described by Oracle as "relatively new."[52]

> A Public Key Infrastructure (PKI) consists of protocols, services, and standards supporting applications of public key cryptography. ***Because the technology is still relatively new***, the term PKI is somewhat loosely defined.

INTRODUCTION TO THE SSL TECHNOLOGY, ORACLE DOCUMENTATION (February 1, 2001), http://docs.oracle.com/cd/E53645_01/tuxedo/docs12cr2/security/publickey.html

179.   The asserted claims do not involve a method of doing business that happens to be implemented on a computer; instead, it involves a method for changing data in a way that will affect the communication system itself, by making it more secure. The security challenges that the '181 patent is directed at overcoming were new and unique to distributed networks, as confirmed in a recent paper from Accenture Services Pvt. Ltd.: "The unprecedented growth of cloud computing has created new security challenges. The problem is ever more complex as there is a transition from traditional computing to a service-based computing."[53]

180.   The '181 patent claims are not directed at a mathematical relationship or formula. The '181 patent claims concrete, specific computer systems and methods for cryptographically protecting and managing access to secure data in multi-party communications.

181.   '181 patent claims transform data from one form into another that will be recognizable by the intended recipient but secure against decryption by unintended recipients.

---

[52] *See also* BACKUPEDGE ENCRYPTION WHITEPAPER, MICROLITE CORPORATION at 2 (2003) (describing the technology of asymmetric keys as "new"); Roger Clarke, MESSAGE TRANSMISSION SECURITY (May 1998), http://www.rogerclarke.com/II/CryptoSecy.html ("Public key cryptography is relatively new and technically complex.").

[53] Deepak Panth, Dhananjay Mehta and Rituparna Shelgaonkar, *A Survey on Security Mechanisms of Leading Cloud Service Providers*, in INTERNATIONAL JOURNAL OF COMPUTER APPLICATIONS 98(1) at 34 (July 2014).

IBM, in its reference guides ("redbooks"), refers to encryption as "transform[ing] data that is

unprotected.

Bertrand Dufrasne and Robert Tondini, IBM DS8870 DISK ENCRYPTION 6th Edition at 4 (2015)
(From a reference guide published by IBM.)

182.   One or more claims of the '181 patent require a specific configuration of

electronic devices, a network configuration, and the use of encryption systems to secure

communications from access by an intermediary. These are meaningful limitations that tie the

claimed methods and systems to specific machines. For example, the below diagram from the

'181 patent illustrates a specific configuration of hardware disclosed in the patent.
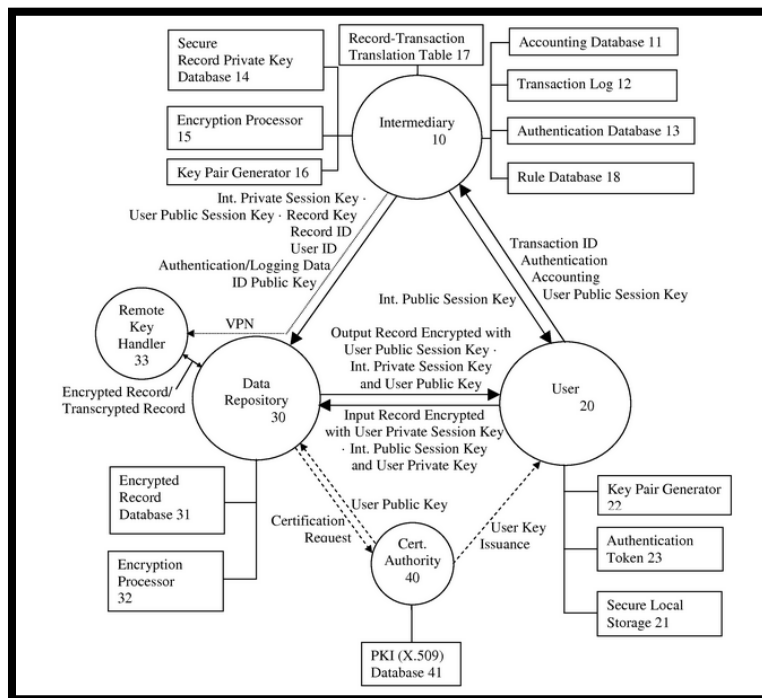
'181 patent, Fig. 1.

5.   U.S. Patent No. 8,566,247

183.   U.S. Patent No. 8,566,247 (the "'247 patent") entitled, System and Method for

Secure Communications Involving and Intermediary, was filed on February 15, 2008 and claims

priority to February 19, 2007. St. Luke is the owner by assignment of the '247 patent. A true

and correct copy of the '247 patent is attached hereto as Exhibit E. The '247 patent claims

specific methods and systems for communicating information which is encrypted from a first

party to a second party, involving an intermediary that selectively authorizes the second party to

comprehend the information, without the intermediary itself being enabled to comprehend the

information, and wherein the asymmetric delivery comprehension function comprises a function

of at least three asymmetric key components of at least three distinct respective asymmetric

delivery comprehension functions.

184.   The '247 patent claims a technical solution to a problem unique to computer

networks – securely transmitting encrypted electronic information via an intermediary device,

wherein the electronic information is cryptographically secure not only from outside attackers,

but also from the intermediary.

185.   The '247 patent has been cited by nineteen issued United States patents and

published patent applications as relevant prior art. Specifically, patents issued to the following

companies have cited the '247 patent.

- General Electric Company
- Microsoft Corporation
- PivotCloud, Inc.
- Futurewei Technologies, Inc.
- Ingenico Group SA
- Telefonaktiebolaget LM Ericsson

186.   At the time of the inventions claimed in the '247 patent, securely communicating

information which is encrypted from a first party to a second party, involving an intermediary,

without the intermediary itself being enabled to comprehend the information presented new and

unique issues over the state of the art. Systems and methods existing at the time the inventions

taught in the '247 patent were conceived, failed to provide for "an intermediary perform[ing] a

requisite function with respect to the transaction without requiring the intermediary to be trusted

with respect to the private information or cryptographic keys for communicated information."
'247 patent, col. 9:8-12.

187.   The '247 patent "provides enhancements to traditional secure communications by providing involvement of a third party, or intermediary, who need not, and preferably does not, have access to the communicated information, while providing transaction-support services between the two parties involved in the communication." '247 patent, col. 9:58-63.

188.   The inventions taught in the '247 patent improve the function of the computer system itself, by making the system more secure.   Researchers at Technische Universität Berlin concluded that securing data from decryption by an intermediary improved the security of computer systems.

> The application of end-to-end encryption **carries security benefits for any solution architecture, e.g., by preventing the access to communication plaintext by intermediaries**. Applying such a security measure is especially meaningful within shared environments, such as public cloud offerings, as those are associated with extensive ramifications of security breaches of those intermediaries, where a potentially large number of tenants would be affected.

Mathias Slawik, et al., *Securing Medical SaaS Solutions Using a Novel End-To-End Encryption Protocol* at 3, in TWENTY SECOND EUROPEAN CONFERENCE ON INFORMATION SYSTEMS (2014).

189.   Although the systems and methods taught in the '247 patent have been adopted by some major corporations, at the time of invention, the technologies taught in the '247 patent claims were innovative and novel. Existing systems dealing with three-party communications "place[d] the third party (or group of third parties) in a position of trust, meaning that the third party or parties, without access to additional information, can gain access to private communications or otherwise undermine transactional security or privacy." '247 patent, col. 1:42-47. Companies such as Oracle recognized that, until recently, security for distributed systems was not a primary concern.[54]

---

[54] *See also* Kevin T. Smith, *Big Data Security: The Evolution of Hadoop's Security Model*, INFOQ (2013) (In 2005 when Hadoop, an open source framework for distributed storage and processing of data sets that is now widely used in the cloud computing instances, "security was not a factor.").

- Security was not a major issue, even for Oracle
  - Standard passwords (scott/tiger, system/manager, ...)
  - Oracle standard users were installed and left open (though not at SAP!)
  - There are some recommendations, but not much more.
  - From Oracle9i, the issue of security was increasingly addressed by Oracle (DBCA: locking of default accounts,..., 10.2: CONNECT roles)

Andreas Becker, *High Security for SAP Data with Oracle Database Vault and Transparent Data Encryption*, ORACLE PRESENTATION 6 (2010).

190.   The '247 patent claims improve upon the functioning of a computer system by allowing encrypted electronic data to be securely transmitted through an intermediary without the intermediary gaining substantial access to the unencrypted information. Further, the inventions disclosed in the '247 patent teach how an intermediary may perform a requisite function with respect to the communication of encrypted information without possessing sufficient information to unilaterally decrypt the encrypted information. The '247 patent teaches ways the intermediary can be used to implement rules (e.g., authenticate access to encrypted information) without placing the intermediary in the position of being able to decrypt the communication. "[B]y exerting this control over the critical function outside the direct communication channel, the intermediary maintains a low communication bandwidth requirement and poses little risk of intrusion on the privacy of the secure communication." '247 patent, col. 9:21-25.This improves the security of the computer system and allows the computer system to operate more efficiently.

191.   The '247 patent claims are not directed to a "method of organizing human activity," "fundamental economic practice long prevalent in our system of commerce," or "a building block of the modern economy." Instead, they are limited to a concretely circumscribed set of methods and systems for communicating information which is encrypted from a first party to a second party, involving an intermediary which selectively authorizes the second party to comprehend the information, without the intermediary itself able to comprehend the information, using an asymmetric delivery comprehension function of the information which is encrypted, different from the associated cryptographic comprehension function.

192.   The '247 patent claims are not directed at the broad concept/idea of "encrypting" or "decrypting" information. Instead, they are limited to a concretely circumscribed set of methods and systems for transmitting encrypted electronic information over a computer network via an intermediary. These methods and systems are technologies unique to the Internet age.

193.   The inventive concepts claimed in the '247 patent are technological, not "entrepreneurial." For example, encrypting from a first party to a second party, involving an intermediary which selectively authorizes the second party to comprehend the information, without the intermediary itself being enabled to comprehend the information is a specific, concrete solution to the technological problem of transferring encrypted information via an intermediary without providing the intermediary substantial access to the information.

194.   Patents cited on the face of the '247 patent identify the problems the '247 patent is directed at solving arising from challenges arising from, and unique to the internet.

> This increase in ***Internet communications has necessitated the development of security systems to insure protection for information transmitted over the Internet.*** Encryption is a basic technique used to scramble information to prevent unsolicited access to that information. One well-known encryption scheme is secret key encryption.

U.S. Patent No. 6,061,448 to Smith (Issued May 9, 2000) (emphasis added).

> Internet-based payment solutions require additional security measures that are not found in conventional POS terminals. This additional requirement is necessitated ***because Internet communication is done over publicly-accessible, unsecured communication line in stark contrast to the private, secure,*** dedicated phone or leased line service utilized between a traditional merchant and an acquiring bank. Thus, it is critical that any solution utilizing the Internet for a communication backbone, employ some form of cryptography.

U.S. Patent No. 6,072,870 to Nguyen (Issued June 6, 2000) (emphasis added).

195.   The '247 patent claims are directed toward a solution rooted in computer technology and use technology unique to computers and computer networking to overcome a problem specifically arising in the realm of secure distributed computing. For example, one or more claims of the '247 patent require information being encrypted with an associated cryptographic comprehension function and the use of at least three asymmetric key components of at least three distinct respective asymmetric delivery comprehension functions so that the second party can

decrypt the encrypted information but an intermediary does not have the ability to decrypt the

information —a result that overrides the routine and conventional sequence of events in

electronic communications, even encrypted electronic communications.

196.   The preemptive effect of the claims of the '247 patent are concretely

circumscribed by specific limitations. For example, claim 10 of the '247 patent requires:

A system for communicating information which is encrypted from a first party to a second party, involving an intermediary that selectively authorizes the second party to comprehend the information, without the intermediary itself being enabled to comprehend the information, comprising:

a communication port which receives information which is encrypted to be communicated or an identification thereof, the information being encrypted with an associated cryptographic comprehension function;

at least one automated processor which conducts a negotiation between the second party and the intermediary through the communication port of an asymmetric delivery comprehension function of the information which is encrypted, different from the associated cryptographic comprehension function, wherein the asymmetric delivery comprehension function comprises a function of at least three asymmetric key components of at least three distinct respective asymmetric delivery comprehension functions, wherein the second party possesses an ability to decrypt the information which is encrypted with the asymmetric delivery comprehension function, and the intermediary possesses a portion of the asymmetric delivery comprehension function which does not impart an ability to decrypt the information which is encrypted;

the at least one automated processor further transforms a comprehension function of the information which is encrypted to be communicated from the associated cryptographic comprehension function to the asymmetric delivery cryptographic comprehension function, comprising using the negotiated asymmetric delivery comprehension function of the at least three key asymmetric key components of the at least three distinct respective asymmetric delivery comprehension functions in an integral process which does not have as an intermediate state a decrypted representation of the information and does not itself require at any time during the transformation, knowledge sufficient for decrypting the information which is encrypted; and

said communication port communicating the information which is encrypted with the asymmetric delivery cryptographic comprehension function to the second party.

197.   The '247 patent does not attempt to preempt every application of the idea of encrypting electronic information transmitted over a computer network, or even the idea of encrypting electronic information transmitted over a computer network via an intermediary.

198.   The '247 patent does not preempt the field of secure third-party communications systems, or prevent use of alternative secure third-party communications systems. For example, the '247 patent includes inventive elements—embodied in specific claim limitations—that concretely circumscribe the patented invention and greatly limit its breadth. These inventive elements are not necessary or obvious tools for achieving secure third-party communications, and they ensure that the claims do not preempt other techniques for secure communications.

199.   For example, the '247 patent describes numerous techniques for secure third-party communications that inform the invention's development but do not, standing alone, fall within the scope of its claims:

- Blind Signatures. *See* David Chaum, "Blind Signatures for Untraceable Payments", Proceedings of Crypto 82, August 1982, p. 199-203. According to the system proposed by David Chaum, a server assists a user in decrypting a message without releasing its secret key or gaining access to the encrypted message.

- Use of a Trusted Intermediary. U.S. Patent No. 6,199,052 to Mitty, describing the use of a trusted intermediary with archive and verification request services for secure electronic transactions.

- Use Of Transaction Certificates. U.S. Patent No. 6,687,822 to Jakobsson, teaching the use of verifiable translation certificates comprising the steps of receiving an input encryption having a first secret key; outputting an output re-encryption of the input encryption, the output re-encryption having a second secret key

- Proxy Key Cryptography. In typical proxy key systems, a proxy receives a private key from a sender of an asymmetrically encrypted message, and a public key from a recipient of the transformed encrypted message, and computes a transform key (e.g., a product of p and q in an RSA type PKI algorithm) which is applied to the asymmetrically encrypted message. *See* Susan Hohenberger, "Advances in Signatures, Encryption, and E-Cash from Bilinear Groups," (Ph.D. Thesis, MIT, May 2006).

200.   Although "[e]ncryption, in general, represents a basic building block of human

ingenuity that has been used for hundreds, if not thousands, of years,"[55] the '247 patent does not

claim, or attempt to preempt, "some process that involves the encryption of data for some

purpose" (or similar abstraction).

201.   The '247 patent does not claim, or attempt to preempt, the performance of an

abstract business practice on the Internet or using a conventional computer.

202.   The claimed subject matter of the '247 patent is not a pre-existing but

undiscovered algorithm.

203.   The '247 patent claims systems and methods that "could not conceivably be

performed in the human mind or pencil and paper."[56]

204.   The '247 patent claims require the use of a computer system.

205.   The claims in the '247 patent require the modifying of data that has concrete and

valuable effects in the field of secure third-party communications. By allowing an intermediary

to receive secure information but not gain access to the unencrypted form of the information, the

'247 patent improves the security of computer systems. Prior art systems that the '247 patent

remedies enabled unauthorized "access to private communications or otherwise undermine[d]

transactional security or privacy." Companies have described the use of encryption in the cloud

as important to improve the security and functioning of systems.

> For many organizations, keeping data private and secure has also become a
> compliance requirement. Standards including Health Insurance Portability and
> Accountability Act of 1996 (HIPAA), Sarbanes-Oxley (SOX), Payment Card

---

[55] *Paone v. Broadcom Corp.,* Case No. 15 CIV. 0596 BMC GRB, 2015 WL 4988279, at *7 (E.D.N.Y. Aug. 19, 2015) (*citing* Fid. Nat'l Info. Servs., Inc., Petitioner, CBM2014-00021, 2015 WL 1967328, at *8 (Apr. 29, 2015) (both upholding the patent eligibility of patents directed toward encryption).

[56] *TQP Dev., LLC v. Intuit Inc.*, Case No. 2:12-CV-180-WCB, 2014 WL 651935, at *4 (E.D. Tex. Feb. 19, 2014) (finding claims directed to encryption to be patent eligible); *see also Paone v. Broadcom Corp.,* Case No. 15 CIV. 0596 BMC GRB, 2015 WL 4988279, at *7 (E.D.N.Y. Aug. 19, 2015); *see also Prism Technologies, LLC v. T-Mobile USA, Inc.*, 12-cv-124, Dkt. No. 428 at 7 (D. Neb. Sept. 22, 2015) (Finding on cross motions for summary judgment that patents directed at delivering resources over an untrusted network were patent eligible. "The problems addressed by Prism's claims are ones that 'arose uniquely in the context of the Internet.'").

Industry Data Security Standard (PCI DSS), the Gramm-Leach-Bliley Act, and EU Data Protection Directives all *require that organizations protect their data at rest and provide defenses against threats*.

HP ATALLA CLOUD ENCRYPTION: SECURING DATA IN THE CLOUD, HP TECHNICAL WHITE PAPER 2 (2014).

206.   The '247 patent claims systems and methods not merely for transferring secure information over a computer network, but for making the computer network itself more secure. [57]

207.   The claimed invention in the '247 claims is rooted in computer technology and overcomes problems specifically arising in the realm of computer networks.

208.   The systems and methods claimed in the '247 patent were not a longstanding or fundamental economic practice at the time of patented inventions. Nor were they fundamental principles in ubiquitous use on the Internet or computers in general.

209.   The asserted claims do not involve a method of doing business that happens to be implemented on a computer; instead, it involves a method for changing data in a way that will affect the communication system itself, by making it more secure. The security challenges that the '247 patent are directed at overcoming were new and unique to distributed networks, as confirmed in a recent paper from Accenture Services Pvt. Ltd.: "The unprecedented growth of cloud computing has created new security challenges. The problem is ever more complex as there is a transition from traditional computing to a service-based computing."[58]

210.   The '247 patent claims are not directed at a mathematical relationship or formula. The '247 patent claims concrete, specific computer systems and methods for cryptographically protecting and managing access to secure data in multi-party communications.

---

[57] Limitations in the prior art that the '247 patent was directed to solving included: computer systems where a "third party plays a requisite role in the transaction but which need not be trusted with access to the information or the cryptographic key" (*Id*., col. 2:6-9); "[p]asswords may be written near access terminals (*Id*. col. 1:52-54);" "[s]ecurity tokens can be stolen or misplaced" (*Id*., col. 1:54-55); and "users may share supposedly secret information" (*Id*., col. 1:55).

[58] Deepak Panth, Dhananjay Mehta and Rituparna Shelgaonkar, *A Survey on Security Mechanisms of Leading Cloud Service Providers*, in INTERNATIONAL JOURNAL OF COMPUTER APPLICATIONS 98(1) at 34 (July 2014).

211.   '247 patent claims transform data from one form into another that will be
recognizable by the intended recipient but secure against decryption by unintended recipients.
IBM, in its reference guides ("redbooks"), refers to encryption as "transform[ing] data that is
unprotected.
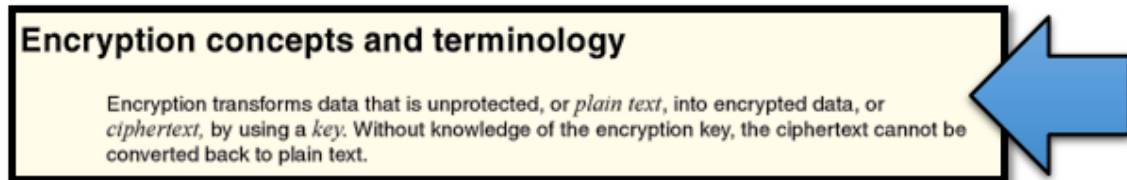
Bertrand Dufrasne and Robert Tondini, IBM DS8870 DISK ENCRYPTION 6th Edition at 4 (2015)
(From a reference guide published by IBM.)

212.   One or more claims of the '247 patent require a specific configuration of
electronic devices, a network configuration, and the use of encryption systems to secure
communications from access by an intermediary. These are meaningful limitations that tie the
claimed methods and systems to specific machines. For example, the below diagram from the
'247 patent illustrates a specific configuration of hardware disclosed in the patent.
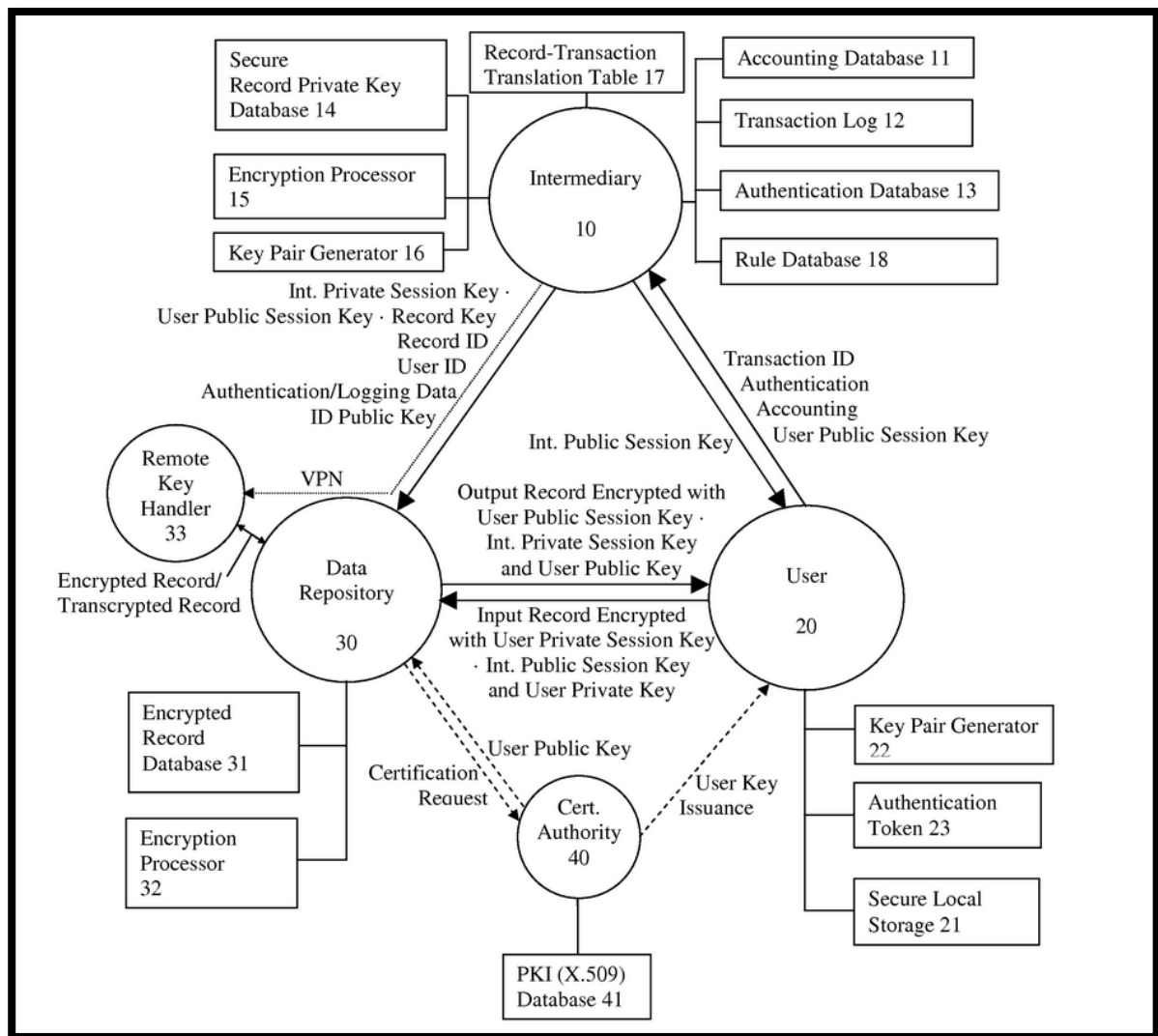
'247 patent, Fig. 1.

C.   Information Record Infrastructure Patents

213.   The IRI patents disclose specific computer based systems and methods for electronically structuring and controlling access to protected data in a plurality of external databases.

214.   Over fifteen years ago, Mr. Felsher conceived of the inventions disclosed in the IRI patents, based on his experiences with the limitations in existing systems for controlling access to electronic medical records and protected electronic data.

215.   During Mr. Felsher's work in the field of electronic medical records, he witnessed

first-hand the drawbacks to existing computer systems and methods for controlling access to

protected data. Existing systems failed to efficiently transmit unstructured protected

information. '368 patent, col. 3:5-10. Other problems included the inability to secure the

protection of data, integrate content management functions, and create a trust infrastructure

wherein an independent third party represents and serves as an agent for the content owner. *Id.*

at col. 3:4-54:16. The result was an inability to effectively manage access to protective data.

The IRI patents disclosed systems and methods that overcome these drawbacks. The inventions

disclosed in the IRI patents improved upon the then-available technology, enabled efficient

access control of unstructured data, reduced costs, and ultimately resulted in a more secure

system.

216.   Apple values systems that provide secure systems and methods for controlling

access to protected data such as the system disclosed in the IRI patents.
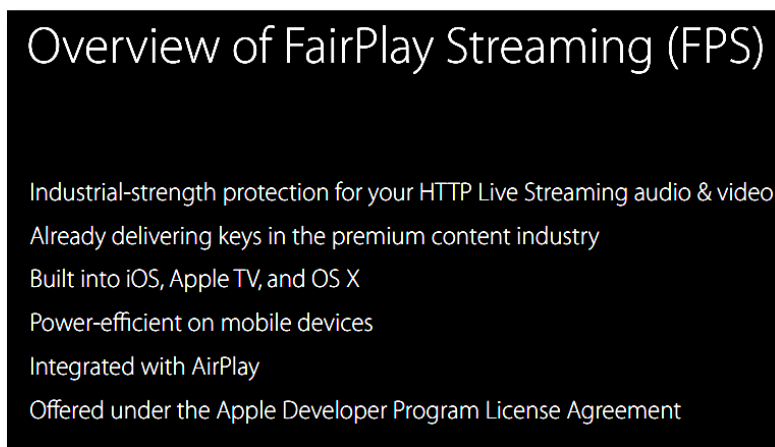
Roger Pantos, *Content Protection for HTTP Live Streaming*, WWDC15 PRESENTATION at 9
(2015).

217.   Apple's competitors, such as Microsoft Corporation and Hewlett Packard

Company, have confirmed the importance and value of systems and methods that manage access

to protected data.

> Today, the need for data protection and security goes well beyond the realm of
> access privileges and firewalls. Organizations of all sizes, in public and private
> sectors, must not only protect information from unauthorized access and intrusion

> but also manage how documents, presentations, spreadsheets, and e-mails are handled in the normal course of daily business

HP INFORMATION RIGHTS MANAGEMENT SOLUTIONS ENSURING LIFE CYCLE PROTECTION OF DIGITAL INFORMATION IN MICROSOFT ENVIRONMENTS, HP WHITE PAPER (2005).

> Such cloud adoption within the healthcare industry is gaining momentum because the economic, clinician productivity and care team collaboration advantages of the cloud are undeniable. However, as was the case for UCHealth, there's *one fundamental concern that continues to weigh heavily on the minds of providers: Is patient data safe, secure and private in the cloud*.

UNIVERSITY OF COLORADO HEALTH ADOPTS MICROSOFT OFFICE 365 FOR ITS DATA PRIVACY AND SECURITY COMMITMENT, MICROSOFT ON THE ISSUES BLOG (December 18, 2013), http://blogs.microsoft.com/on-the-issues/2013/12/18/university-of-colorado-health-adopts-microsoft-office-365-for-its-data-privacy-and-security-commitment/ (emphasis added).

218.   Academics have confirmed the value of secure information access management

systems such as the inventions disclosed in the IRI patents.

> *With the proliferation of the Internet, the speed and ease of digital data exchange has increased, together with the number of potential parties that can exchange data*. This has also meant that digital data security is no longer confined to the computer that holds the original data, or even behind corporate firewalls. Furthermore, data security no longer applies only to the access to data, but also to what the user can do with the data

Alapan Arnab and Andrew Hutchinson, *Digital Rights Management - An Overview of Current Challenges and Solutions*, in PROCEEDINGS OF INFORMATION SECURITY SOUTH AFRICA CONFERENCE (2004) (emphasis added).[59]

219.   Although major corporations offer systems for providing secure access to

protected data today, at the time the inventions disclosed in the IRI patents were conceived,

systems had significant limitations that were addressed by the inventions disclosed in the IRI

patents.

> While "awareness of risks and of possible technical solutions is increasing," the authors would appear to be describing a rather precarious environment, at least in the short run. The picture does not improve when one focuses on the details of some of the technical fixes. Barrows and Clayton deem "tight" prospective access restrictions—a "need to know," mandatory access control model—as largely incompatible with the dynamic health care environment.

---

[59] *See also* Murat Kantarcioglu, Wei Jiang, and Bradley Malin, *A Privacy-Preserving Framework for Integrating Person-Specific Databases* at 299, PRIVACY IN STATISTICAL DATABASES LNCS 5262 (2008) (Describing the difficulty in managing medical records stored in multiple electronic databases "in the healthcare realm, patients are mobile and their data can be collected by multiple locations, such as when a patient visits one hospital for primary care and a second hospital to participate in a clinical trial.").

Reid Cushman, *Serious Technology Assessment for Health Care Information Technology*, JOURNAL OF THE AMERICAN MEDICAL INFORMATICS ASSOCIATION 4(4) (1997).[60]

220.   The claims in the IRI patents describe solutions that are rooted in computer technology to overcome problems specific to and characteristic of complex computer networks where protected data is stored. For example, academics identified distributed information systems as leading to new problems regarding information rights management that the IRI patents solve.

> The development and wider use of wireless networks and mobile devices has led to novel pervasive computing environments **which pose new problems for software rights management** and enforcement on resource-constrained and occasionally connected devices. . . . The latter opens new channels for super-distribution and sharing of software applications that do not impose a cost on the user.

Ivana Dusparic, Dominik Dahlem, and Jim Dowling, *Flexible Application Rights Management in a Pervasive Environment*, in IEEE INTERNATIONAL CONFERENCE ON E-TECHNOLOGY, E-COMMERCE AND E-SERVICE, pages 680–685 (2005) (emphasis added).[61]

> Then there is the cloud. Cloud, cloud, cloud, it's on every webcast, in every article. The cloud has many advantages. Why wouldn't you want to outsource all

---

[60] This reference is cited on the face of the IRI patents as an exemplar illustrating limitations in systems existing at the time the inventions disclosed in the IRI patents were conceived; *see also* Alapan Arnab and Andrew Hutchinson, *Digital Rights Management - An Overview of Current Challenges and Solutions*, in PROCEEDINGS OF INFORMATION SECURITY SOUTH AFRICA CONFERENCE (2004) (emphasis added) ("none of these products provide for all the needs of an enterprise, and furthermore these products do not offer all the benefits that DRM potentially offers to an enterprise).

[61] *See also* Aaron Franks, Stephen LaRoy, Miek Wood, and Mike Worth. *Idrm: An Analysis Of Digital Rights Management For The Itunes Music Store*, TECHNICAL REPORT, UNIVERSITY OF BRITISH COLUMBIA (2005) ("The need for secure digital rights management (DRM) is more urgent today than ever before. With the rapid increase in broadband availability, Internet file sharing has become a threat to content providers' bottom line."); Mike Godwin, *What Every Citizen Should Know About DRM, A.K.A. 'Digital Rights Management*,' PUBLIC KNOWLEDGE (2004) ("As circumvention tools evolve, and as new technologies pose new infringement problems, the locking of industrial sectors into a particular "standard" scheme, mediated and supervised by government, actually slows the ability of the content sector to respond to new problems.); HP DIGITAL RIGHTS MANAGEMENT (DRM) FOR NETWORK AND SERVICE PROVIDERS (NSPS), HP SOLUTION BRIEF (2003) ("DRM [Digital Rights Management] is an emerging technology with fragmented addressable markets, solution capabilities and standards."); Arun Kulkarni, Harikrisha Gunturu, and Srikanth Datla, *Association-Based Image Retrieval* at 183, WSEAS TRANS. SIG. PROC.Vol.4(4) (April 2008) ("With advances in computer technology and the World Wide Web there has been an explosion in the amount and complexity of multimedia data that are generated, stored, transmitted, analyzed, and accessed.").

your costs of network management, storage, system administration?   The cloud
makes perfect sense but has one massive concern... security.

Simon Thorpe, *Security in the Enterprise 2.0 World: Conflicts of Collaboration*, ORACLE
OFFICIAL BLOG, September 27, 2010, https://blogs.oracle.com/irm/.

221.   Although secure and effective information rights management, in some form, has

been an objective of corporations and researchers for many years ('368 patent, col. 6:61-7:3), the

IRI patents are directed at solving problems that are unique to the realm of computers and

specifically network cloud computing.

222.   The systems and methods disclosed in the IRI patents have particular application

to two primary fields: electronic medical records and electronic rights management.

Shortcomings in available technology at the time the inventions disclosed in the IRI patents were

conceived, led to the development of the IRI patents.

223.   A brief overview of the state of the prior art in these two areas provides context to

understanding the truly inventive nature of the IRI patents. The specific systems and methods

disclosed and claimed in the IRI patents are discussed in detail later in this Complaint.

224.   Background on the state of the art at the time of the inventions disclosed in the

IRI patents confirms that the patented inventions are limited to specific computer systems and

methods and address issues specific to accessing protected data using modern computer

networks.

225.   ***Information Rights Management***. The inventions disclosed in the IRI patents

have particular application to the management of rights in digital works, to allow a content

owner to exploit the value of the works while assuring control over the use and dissemination.

The IRI patents address problems specific to and arising from distribution and protected works

on the internet.

226.   At the time the inventions disclosed in the IRI patents were conceived, the growth

of the internet created unique problems relating to managing rights to protected works.

There's too much data being collected in so many ways, and a lot of it in ways
that you don't feel you had a role in the specific transaction," he [Craig Mundie]
said. "Now that you're just being observed, whether it's for commercial purposes
or other activities, ***we have to move to a new model.*** . . .   Under the model

imagined by Mundie [a] central authority would distribute encryption keys to applications, allowing them to access protected data in the ways approved by the data's owners.

Tom Simonite, *Microsoft Thinks DRM Can Solve the Privacy Problem*, MIT TECHNOLOGY REVIEW, October 10, 2013 (emphasis added) (Craig Mundie is Senior Advisor to the CEO at Microsoft and its former Chief Research and Strategy Officer).[62]

227.   In the late 1990s and early 2000s, information rights management systems had significant limitations. Prior art systems did not create a trust infrastructure, wherein an independent third party represents and serves as agent for the content owner, implementing a set of restrictive rules for use of the content, and interacting and servicing customers.

228.   Apple's iTunes software, released in January 2001, was indicative of the state of information rights management systems available at the time. Apple's 2001 iTunes release lacked information rights management software and was marketed to users who wanted to convert compact discs into MP3s. The product was marketed with the tagline "Rip. Mix. Burn."[63]
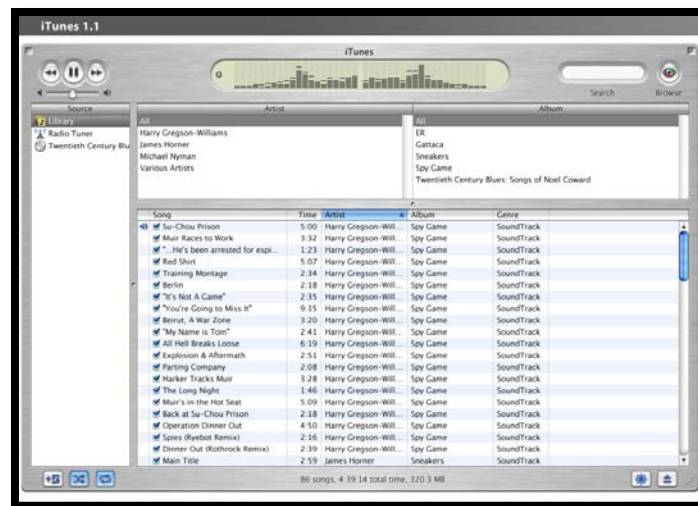
Screenshot of Apple's iTunes 1.1 Program (released in January 2001).

---

[62] *See also* Martin Abrahams, *Document Theft - IRM as a Last Line of Defense*, ORACLE IRM, THE OFFICIAL BLOG, August 1, 2011, https://blogs.oracle.com/irm/ ("The relevance of IRM is clear. . . . In a cloudy world, where perimeters are of diminishing relevance, you need to apply controls to the assets themselves.").

[63] Jacqui Cheng, *iTunes Through The Ages: We Look Back At 12 Years Of iTunes Releases*, ARS TECHNICA, May 23, 2012, http://arstechnica.com/apple/2012/11/itunes-through-the-ages/.

229.   Rudimentary information rights management systems such as Microsoft's

PlayForSure and RealNetwork's Rhapsody were still years from being released. Even when

these systems were released in 2004 they had significant limitations. Both systems lacked the

ability of a third party to act as an intermediary between a content creator and a user. The state

of the art at the time the inventions disclosed in the IRI patents were conceived underscores the

inventive nature of the IRI patents.

230.   ***Electronic Medical Records***. The IRI patents disclose systems and methods for

controlling access to protected health information where the information is stored in one or more

external databases. Systems for controlling access to medical records, contemporaneous to the

IRI patents had significant limitations that the IRI patents address.[64] These systems included: (1)

Anonymizing Records. A method used in contemporaneous systems to the IRI patents is the

maintenance of anonymous medical records. However, anonymizing techniques did not provide

patients and medical professionals the ability to access patient specific records. (2) Indexing.

Systems contemporaneous to the IRI patents indexed medical records with anonymous

identification codes.[65] While these systems preserved privacy, these systems made locating a

database record other than by patient identifier, or its accession identifier, difficult. (3) Proxy

Systems. Other contemporaneous systems used a proxy server to protect user privacy.

---

[64] *See* Reid Cushman, *Serious Technology Assessment for Health Care Information Technology*, J. AM. MED. INFORM. ASSOC. 4: 259-265 (1997) (This article is cited on the face of the IRI patents and finds "Data protection practices in the typical late twentieth-century organization are not very good, even in putatively "secure" institutions. . . The forthcoming study of health care security by the National Academy of Sciences, to be released in February 1997, is expected to reach a similar conclusion. The widespread deficits in security are hardly a secret; they are common fodder among information systems professionals."); *see also* Bhavani Thuraisingham, *Data and Applications Security: Developments and Directions* at 2, PROCEEDINGS IEEE COMPSAC (2002) (Discussing issues with electronic medical records "There are numerous security issues for such systems including secure information sharing and collaboration. Furthermore, data is no longer only in structured databases. . . . Security for such data has not received much attention.").

[65] *See also* Murat Kantarcioglu and Chris Clifton, *Security Issues in Querying Encrypted Data* at 2, TECHNICAL REPORT CSD TR 04-013, Purdue University Computer Sciences Department (2004) ("methods that quantize or "bin" values reveal data distributions. Methods that hide distribution, but preserve order, can also disclose information if used naively").

However, systems using an Internet proxy resulted in a loss of rights and did not act in a representative capacity for the content owner, and did not integrate content management functions.

231.   In addition, access to these early medical records systems was limited to authorized individuals who were on-site, as these systems provided little-to-no connectivity to anyone outside of the organization or to the Internet generally. Because access was restricted to on-site users on a local network using stationary terminals in designated areas, there was very little emphasis placed on data security.

232.   In sharp contrast to the flexible, modular, and tightly integrated multi-layer security and access control framework disclosed and claimed in the IRI patents, systems such as Epic System Corporation's CareWeb[66] had significant limitations, including: inability to effectively control access on a record-by-record basis within respective external databases, as claimed in several IRI patents; inability to distinguish between records within an external or backend database, the databases accessed through CareWeb were basically opaque to the "CareWeb" system; and CareWeb's fixed structure was expressly limited to a particular, monolithic front-end architecture for secure implementation.

233.   At the time the inventions disclosed in the IRI patents were conceived, the medical community showed little sign of implementing a system for controlling access to medical records that were stored in extern databases. Further, computer networks presented new challenges and unique problems that the IRI patents addressed.

---

[66] John D. Halamka, Peter Szolovits, David Rind, and Charles Safran, *A WWW Implementation of National Recommendations for Protecting Electronic Health Information*, J. AM. MED. INFORM. ASSOC. 4: 458-464 (1997) (The limitations of the CareWeb system are discussed in depth in the specification of the IRI patents.).

> As health care moves from paper to electronic data collection, providing easier access and dissemination of health information, the development of guiding privacy, confidentiality, and security principles is necessary to help balance the protection of patients' privacy interests against appropriate information access. . . . It is imperative that all participants in our health care system work actively toward a viable resolution of this information privacy debate.

Suzy Buckovich, Helga Rippen, and Michael Rozen, *Driving Toward Guiding Principles: A Goal for Privacy, Confidentiality, and Security of Health Information*, J. AM. MED. INFORM. ASSOC. 6 (1999).

234.   The need for a secure system for providing access to medical records was specifically required in the cloud computing context where medical records were stored in one or more external databases.

> The healthcare industry is in a major period of transformation and IT modernization. More than ever, healthcare providers and professionals are faced with the need to be more efficient, reduce costs and collaborate seamlessly as virtual teams to deliver higher quality care for more people at a lower cost point. Healthcare organizations are increasingly looking to cloud technologies to help them meet these goals. However, a natural concern with using cloud technology is keeping sensitive health information private and secure.

Hemant Pathak, DATA PRIVACY AND COMPLIANCE IN THE CLOUD IS ESSENTIAL FOR THE HEALTHCARE INDUSTRY (December 2013), http://www.microsoft.com/en-us/health/blogs/data-privacy-and-compliance-in-the-cloud-is-essential-for-the-healthcare-industry/default.aspx.

235.   On information and belief, contemporaneous to, and following conception of the inventions disclosed in the IRI patents, Texas educational institutions, Texas governmental entities, and businesses headquartered in Texas actively entered the field of electronically structuring and controlling access to protected health data stored in a plurality of external databases. In 2006, Texas Gov. Rick Perry called for widespread adoption of health information technology ("HIT").[67] Governor Perry signed Senate Bill 45, which created the Health Information Technology Advisory Committee (HITAC) within the Texas Statewide Health Coordinating Council in the Department of State Health Services.[68] In addition, various

---

[67] Gov. Rick Perry, *State-of-the-State Speech*; February 6, 2007, http://governor.state.tx.us/news/speech/5567/

[68] Texas Senate Bill 45, Texas 79th Regular Legislative Session (25 TAC §§571.11-571.13); s*ee also* Texas Executive Order RP-61*, Relating to the Creation, Composition, and Operation of the Governor's Health System Integrity Partnership for the State of Texas* (October 9, 2006) (The Partnership was directed to develop a method for secure exchange of electronic health information.).

universities studied and implemented systems for securely managing access to distributed medical records.[69]

236.   Texas based companies incorporated systems and methods for electronically structuring and controlling access to protected data in a plurality of external databases into numerous products. Many of these same companies cite the IRI patents in their own patents. Texas based businesses that developed products/technologies incorporating these technologies included: HP Enterprise Services, LLC of Plano, Texas; Hospitalists Now, Inc. of Austin, Texas; StandardCall, LLC of Frisco, Texas; Security First Corp whose inventors were based in various locations in Texas; Huawei Technologies Co., Ltd. of Plano, Texas; Omnyx LLC whose inventors included individuals based in Texas; Electronic Data Systems Corporation of Plano, Texas, South Texas Accelerated Research Therapeutics, LLC of San Antonio, Texas; etc.

1.   **U.S. Patent No. 7,587,368**

237.   U.S. Patent No. 7,587,368 (the "'368 patent") entitled, Information Record Infrastructure, System and Method, was filed on July 5, 2001, and claims priority to July 6, 2000. St. Luke is the owner by assignment of the '368 patent. A true and correct copy of the '368 patent is attached hereto as Exhibit F. The '368 patent claims specific methods and systems for securely controlling access to a plurality of digital records by a remote computer.

238.   The '368 patent has been cited by over 100 United States patents and patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the '368 patent as relevant prior art.

- Microsoft Corporation
- LG Electronics, Inc.
- Canon Kabushiki Kaisha
- Hewlett-Packard Development Company, L.P.
- Voltage Security, Inc.
- Northrop Grumman Systems Corporation
- International Business Machines Corporation
- Mcafee, Inc.

---

[69] *See* David E. Gerber et al., Predictors and Intensity of Online Access to Electronic Medical Records Among Patients with Cancer, J Oncol Pract. Vol. 10(5) (Sept. 2014) (studying electronic medical record infrastructure implementations at and Texas hospitals);

- J.D. Power And Associates
- NEC Corporation
- Electronics And Telecommunications Research Institute (ETRI)
- Koninkliike Philps Electronics N.V.
- Huawei Technologies Co., Ltd.
- Ricoh Co., Ltd.
- Massachusetts Institute Of Technology

239.   The '368 patent claims a technical solution to a problem unique to computer networks – securely transmitting encrypted digital records and controlling access to digital records requested by a remote computer.

240.   At the time of the inventions claimed in the '368 patent, electronically structuring and controlling access to protected data in a plurality of external databases presented new and unique issues over the state of the art. As explained in the '368 patent: "The present invention therefore seeks to provide a comprehensive set of technologies to address the full scope of issues presented in implementing a secure and versatile information content infrastructure that respects the rights of content owners and users to privileges, such as confidentiality." '368 patent, col. 54:27-33.

241.   Although the systems and methods taught in the '368 patent have been adopted by leading businesses today, at the time of invention, the technologies taught in the '368 patent claims were innovative and novel. "Existing systems do not create a trust infrastructure, wherein an independent third party represents and serves as an agent for the content owner, implementing a set of restrictive rules for use of content . . . Thus, existing intermediaries do not act in a representative capacity for the content owner, and do not integrate content management functions." '368 patent, col. 5:4-16.

242.   Further, the '368 patent claims improve upon the functioning of a computer system by allowing encrypted electronic data to be securely transmitted through an intermediary. This improves the security of the computer system and allows it to be more efficient. "[B]y consolidating a plurality of institutions [referring to digital records stored in external databases], uniformity, interoperability, cost reductions, and improved security result." '368 patent, col. 67:65-67.

243.   The '368 patent claims are not directed to a "method of organizing human activity," "fundamental economic practice long prevalent in our system of commerce," or "a building block of the modern economy." Instead, they are limited to a concretely circumscribed set of methods and systems that provide a conduit for the authorized transmission of digital records, while maintaining the security of the records against unauthorized access.

244.   The '368 patent claims are not directed at the broad concept/idea of "managing digital records." Instead, the '368 patent claims are limited to a concretely circumscribed set of methods and systems for authorizing and transmitting secure digital records. These methods and systems are technologies unique to the Internet age.

245.   The '368 patent claims are directed toward a solution rooted in computer technology and use technology unique to computers and computer networking to overcome a problem specifically arising in the realm of secure distributed computing. For example, one or more claims of the '368 patent require encrypting and sending, by the server system, the requested digital record which has been validated, using the public key and the session key to encrypt the digital record - a procedure that overrides the routine and conventional sequence of events in electronic communications, even encrypted electronic communications.

246.   The '368 patent is directed to specific problems in the field of digital record access and transmission.

247.   The preemptive effect of the claims of the '368 patent are concretely circumscribed by specific limitations. For example, claim 1 of the '368 patent requires:

A method, comprising the steps of:

storing a plurality of digital records and respective access rules for each digital record in a computer memory associated with a server system;

receiving a request for access, from a remote computer, to access a digital record stored in the computer memory;

validating, by the server system, the received request to access the digital record by applying a respective set of access rules for the digital record stored in the computer memory;

retrieving, by the server system, a public key having an associated private key, and associating a logging wrapper having a respective

session key with the digital record, after validating the received request, wherein the session key is distinct from the public key and the private key;

encrypting and sending, by the server system, the requested digital record which has been validated, using the public key and the session key to encrypt the digital record;

receiving and decrypting the encrypted digital record, by the remote computer, using the private key, and the session key in conjunction with the logging wrapper;

generating by the logging wrapper, at the remote computer, a logging event; and

recording the logging event in an access log.

248.   The '368 patent does not attempt to preempt every application of the idea of controlling access to an encrypted digital record over a computer network.

249.   The '368 patent does not preempt the field of electronically structuring and controlling access to protected data in a plurality of external databases. For example, the '368 patent includes inventive elements—embodied in specific claim limitations—that concretely circumscribe the patented invention and greatly limit its breadth. These inventive elements are not necessary or obvious tools for achieving secure third-party communications, and they ensure that the claims do not preempt other techniques for secure communications.

250.   For example, the '368 patent describes numerous techniques for electronically structuring and controlling access to protected data in a plurality of external databases. The techniques inform the invention's development but do not, standing alone, fall within the scope of its claims:

- Rights-Based Access to Database Records. U.S. Pat. No. 5,325,294 to Keene, relates to a system that receives and stores the individual's medical information, after the individual is tested to establish this information and the date on which such information was most recently obtained.

- Security Tokens. U.S. Patent No. 5,978,918 to Scholnick, discloses a back-end process returns a time sensitive token that the "sender" sends to the "receiver." The "receiver" takes the time sensitive token and uses it to retrieve the private data.[70]

---

[70] *See also* Arindam Khaled et al., *A Token-based Access Control System for RDF Data in the Clouds* at 104,.in PROCEEDINGS OF THE 2ND IEEE INTERNATIONAL CONFERENCE ON CLOUD

- Role-Based Access. U.S. Pat. No. 6,023,765 to Kuhn, relates to a role-based access control in multi-level secure systems.

- Secure Networks. U.S. Pat. No. 5,579,393 to Conner, relates to a system and method for secure digital records, comprising a provider system and a payer system.

- Cryptographic Technology. U.S. Pat. No. 5,956,408 to Arnold, relates to an apparatus and method for secure distribution of data. Data, including program and software updates, is encrypted by a public key encryption system using the private key of the data sender.

- Watermarking. U.S. Pat. No. 5,699,427 to Chow, relates to a method to deter document and intellectual property piracy through individualization, and a system for identifying the authorized receiver of any particular copy of a document.

- Computer System Security. U.S. Pat. No. 5,881,225 to Worth, relates to a security monitor for controlling functional access to a computer system. A security monitor controls security functions for a computer system. A user desiring access to the system inputs a user identification and password combination, and a role the user to assume is selected from among one or more roles defined in the system.

- Computer Security Devices. U.S. Pat. No. 5,982,520 to Weiser, relates to a personal storage device for receipt, storage, and transfer of digital information to other electronic devices has a pocket sized crush resistant casing with a volume of less than about ten cubic centimeters.

- Computer Network Firewall. U.S. Pat. No. 5,944,823 to Jade, relates to a system and method for providing outside access to computer resources through a firewall. A firewall isolates computer and network resources inside the firewall from networks, computers and computer applications outside the firewall.

- Virtual Private Network. U.S. Pat. No. 6,079,020 to Liu, relates to a method and an apparatus for managing a virtual private network operating over a public data network. This public data network has been augmented to include a plurality of virtual private network gateways so that communications across the virtual private network are channeled through the virtual private network gateways.

COMPUTING TECHNOLOGY AND SCIENCE (2010) (discussing the use of a "token-based access control system . . . implemented in Hadoop (an open source cloud computing framework)").

- Biometric Authentication. U.S. Pat. No. 5,193,855 to Shamos relates to a patient and healthcare provider identification system which includes a database of patient and healthcare provider information including the identity of each patient and provider and some identification criteria (such as fingerprint data).[71]

251.   Although "[e]ncryption, in general, represents a basic building block of human ingenuity that has been used for hundreds, if not thousands, of years,"[72] the '368 patent does not claim, or attempt to preempt, "some process that involves the encryption of data for some purpose" (or similar abstraction).

252.   The '368 patent does not claim, or attempt to preempt, the performance of an abstract business practice on the Internet or using a conventional computer.

253.   The claimed subject matter of the '368 patent is not a pre-existing but undiscovered algorithm.

254.   The '368 patent claims systems and methods that "could not conceivably be performed in the human mind or pencil and paper."[73]

255.   The '368 patent claims require the use of a computer system.

256.   The '368 patent claims systems and methods not merely for transferring secure information over a computer network, but for making the computer network itself more secure.

---

[71] Nary Subramanian, *Biometric Authentication*, in ENCYCLOPEDIA OF CRYPTOGRAPHY AND SECURITY (S. Jajodia and H.C.A. van Tilborg 2nd ed. 2011) ("Biometric authentication is a technique for identifying the person accessing a secured asset . . . by comparing their unique biological features . . . [an] issue with biometric authentication is privacy of personal data.").

[72] *Paone v. Broadcom Corp.,* Case No. 15 CIV. 0596 BMC GRB, 2015 WL 4988279, at *7 (E.D.N.Y. Aug. 19, 2015) (*citing Fid. Nat'l Info. Servs., Inc.*, Petitioner, CBM2014-00021, 2015 WL 1967328, at *8 (Apr. 29, 2015) (both upholding the patent eligibility of patents directed toward encryption).

[73] *TQP Dev., LLC v. Intuit Inc.*, Case No. 2:12-CV-180-WCB, 2014 WL 651935, at *4 (E.D. Tex. Feb. 19, 2014) (finding claims directed to encryption to be patent eligible); *see also Paone v. Broadcom Corp.,* Case No. 15 CIV. 0596 BMC GRB, 2015 WL 4988279, at *7 (E.D.N.Y. Aug. 19, 2015); *see also Prism Technologies, LLC v. T-Mobile USA, Inc.*, 12-cv-124, Dkt. No. 428 at 7 (D. Neb. Sept. 22, 2015) (Finding on cross motions for summary judgment that patents directed at delivering resources over an untrusted network were patent eligible. "The problems addressed by Prism's claims are ones that 'arose uniquely in the context of the Internet.'").

257.   The claimed invention in the '368 claims is rooted in computer technology and overcomes problems specifically arising in the realm of computer networks.

258.   The systems and methods claimed in the '368 patent were not a longstanding or fundamental economic practice at the time of patented inventions. Nor were they fundamental principles in ubiquitous use on the Internet or computers in general.

259.   The asserted claims do not involve a method of doing business that happens to be implemented on a computer; instead, it involves a method for changing digital records in a way that will affect the communication system itself, by making it more secure.

260.   One or more claims of the '368 patent require a specific configuration of electronic devices, a network configuration, and the use of encryption systems to secure communications and manage access to secure digital records. These are meaningful limitations that tie the claimed methods and systems to specific machines. For example, the below diagram from the '368 patent illustrates a specific configuration of hardware disclosed in the patent.
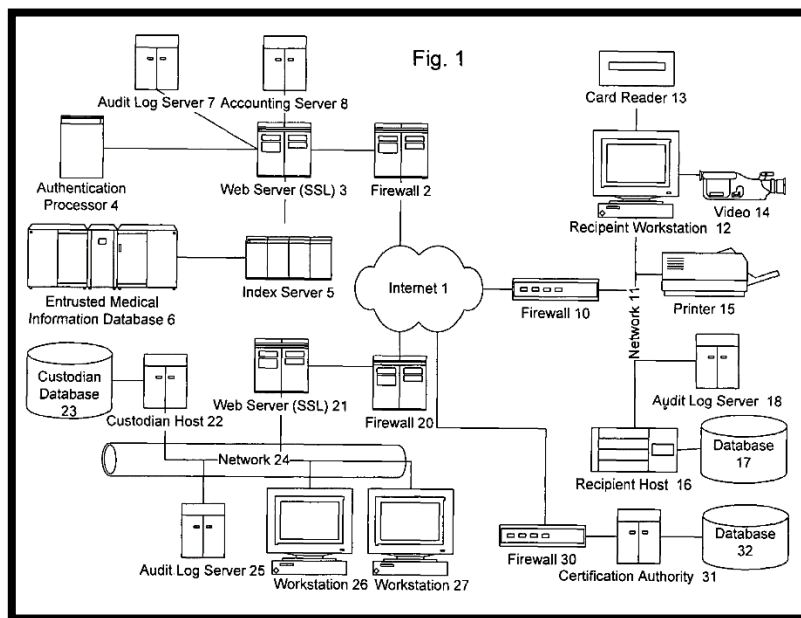
'368 patent, Fig. 1.

2.   U.S. Patent No. 8,498,941

261.   U.S. Patent No. 8,498,941 (the "'941 patent") entitled, Information Record Infrastructure, System and Method, was filed on July 22, 2009, and claims priority to July 6, 2000. St. Luke is the owner by assignment of the '941 patent. A true and correct copy of the '941 patent is attached hereto as Exhibit G. The '941 patent claims specific methods and systems for securely controlling access to a plurality of digital records by a remote computer where each record has associated access rules.

262.   The '941 patent has been cited by 10 United States patents and patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the '941 patent as relevant prior art.

- Red Hat, Inc.
- Intuit, Inc.
- Microsoft Corporation
- Silver Spring Networks, Inc.
- Royal Canadian Mint
- Extendabrain Corporation

263.   The '941 patent claims a technical solution to a problem unique to computer networks – controlling access to a plurality of records provided within a plurality of automated electronic databases, each record having an associated set of access rules.

264.   At the time of the inventions claimed in the '941 patent, electronically structuring and controlling access to protected data in a plurality of external databases presented new and unique issues over the state of the art. As explained in the '941 patent: "The present invention therefore seeks to provide a comprehensive set of technologies to address the full scope of issues presented in implementing a secure and versatile information content infrastructure that respects the rights of content owners and users to privileges, such as confidentiality." '941 patent, col. 53:35-39.

265.   Although the systems and methods taught in the '941 patent have been adopted by leading businesses today, at the time of invention, the technologies taught in the '941 patent claims were innovative and novel. "Existing systems do not create a trust infrastructure, wherein an independent third party represents and serves as an agent for the content owner, implementing

a set of restrictive rules for use of content . . . Thus, existing intermediaries do not act in a representative capacity for the content owner, and do not integrate content management functions." '941 patent, col. 5:17-20.

266.   Further, the '941 patent claims improve upon the functioning of a computer system by allowing encrypted electronic data to be securely transmitted through an intermediary. This improves the security of the computer system and allows it to be more efficient. "[B]y consolidating a plurality of institutions [referring to digital records stored in external databases], uniformity, interoperability, cost reductions, and improved security result." '941 patent, col. 66:21-23.

267.   The '941 patent claims are not directed to a "method of organizing human activity," "fundamental economic practice long prevalent in our system of commerce," or "a building block of the modern economy." Instead, they are limited to a concretely circumscribed set of methods and systems that provide a conduit for the authorized transmission of digital records, while maintaining the security of the records against unauthorized access.

268.   The '941 patent claims are not directed at the broad concept/idea of "managing digital records." Instead, the '941 patent claims are limited to a concretely circumscribed set of methods and systems for authorizing and transmitting secure digital records. These methods and systems are technologies unique to the Internet age.

269.   The '941 patent claims are directed toward a solution rooted in computer technology and use technology unique to computers and computer networking to overcome a problem specifically arising in the realm of secure distributed computing. For example, one or more claims of the '941 patent require the generation of an information polymer - a procedure that overrides the routine and conventional sequence of events in electronic communications, even encrypted electronic communications.

270.   The '941 patent is directed to specific problems in the field of digital record access and transmission.

271.   The preemptive effect of the claims of the '941 patent are concretely circumscribed by specific limitations. For example, claim 1 of the '941 patent requires:

A method for controlling access to a plurality of records provided within a plurality of automated electronic databases, each record having an associated set of access rules, comprising:

receiving a request from a requestor, the requestor having at least one attribute;

searching the plurality of automated electronic databases to find records in dependence on the request and on connections between respective records;

applying a set of access rules associated with each found record by at least one automated processor, to produce a set of accessible records;

linking the set of accessible records into an information polymer using a server device;

applying at least one compensation rule by at least one automated processor, dependent on the at least one attribute of the requestor;

logging at least the request for access by at least one automated processor; and

communicating the information polymer to the requestor.

272.   The '941 patent does not attempt to preempt every application of the idea of controlling access to a digital record over a computer network where the digital records are within a plurality of automated electronic databases.

273.   The '941 patent does not preempt the field of electronically structuring and controlling access to protected data in a plurality of external databases. For example, the '941 patent includes inventive elements—embodied in specific claim limitations—that concretely circumscribe the patented invention and greatly limit its breadth. These inventive elements are not necessary or obvious tools for achieving secure third-party communications, and they ensure that the claims do not preempt other techniques for secure communications.

274.   For example, the '941 patent describes numerous techniques for electronically structuring and controlling access to protected data in a plurality of external databases. The

techniques inform the invention's development but do not, standing alone, fall within the scope

of its claims:

- Rights-Based Access to Database Records. U.S. Pat. No. 5,325,294 to Keene, relates to a system that receives and stores the individual's medical information, after the individual is tested to establish this information and the date on which such information was most recently obtained

- Role-Based Access. U.S. Pat. No. 6,023,765 to Kuhn, relates to a role-based access control in multi-level secure systems.

- Security Tokens. U.S. Patent No. 5,978,918 to Scholnick, discloses a back-end process returns a time sensitive token that the "sender" sends to the "receiver." The "receiver" takes the time sensitive token and uses it to retrieve the private data.[74]

- Secure Networks. U.S. Pat. No. 5,579,393 to Conner, relates to a system and method for secure digital records, comprising a provider system and a payer system.

- Cryptographic Technology. U.S. Pat. No. 5,956,408 to Arnold, relates to an apparatus and method for secure distribution of data. Data, including program and software updates, is encrypted by a public key encryption system using the private key of the data sender.

- Watermarking. U.S. Pat. No. 5,699,427 to Chow, relates to a method to deter document and intellectual property piracy through individualization, and a system for identifying the authorized receiver of any particular copy of a document.

- Computer System Security. U.S. Pat. No. 5,881,225 to Worth, relates to a security monitor for controlling functional access to a computer system. A security monitor controls security functions for a computer system. A user desiring access to the system inputs a user identification and password combination, and a role the user to assume is selected from among one or more roles defined in the system.

- Computer Security Devices. U.S. Pat. No. 5,982,520 to Weiser, relates to a personal storage device for receipt, storage, and transfer of digital information to other electronic

---

[74] *See also* Arindam Khaled et. al, *A Token-based Access Control System for RDF Data in the Clouds* at 104,.in PROCEEDINGS OF THE 2ND IEEE INTERNATIONAL CONFERENCE ON CLOUD COMPUTING TECHNOLOGY AND SCIENCE (2010) (discussing the use of a "token-based access control system . . . implemented in Hadoop (an open source cloud computing framework)").

devices has a pocket sized crush resistant casing with a volume of less than about ten cubic centimeters.

- Computer Network Firewall. U.S. Pat. No. 5,944,823 to Jade, relates to a system and method for providing outside access to computer resources through a firewall. A firewall isolates computer and network resources inside the firewall from networks, computers and computer applications outside the firewall.

- Virtual Private Network. U.S. Pat. No. 6,079,020 to Liu, relates to a method and an apparatus for managing a virtual private network operating over a public data network. This public data network has been augmented to include a plurality of virtual private network gateways so that communications across the virtual private network are channeled through the virtual private network gateways.

- Biometric Authentication. U.S. Pat. No. 5,193,855 to Shamos relates to a patient and healthcare provider identification system which includes a database of patient and healthcare provider information including the identity of each patient and provider and some identification criteria (such as fingerprint data).[75]

275.   The '941 patent does not claim, or attempt to preempt, the performance of an abstract business practice on the Internet or using a conventional computer.

276.   The claimed subject matter of the '941 patent is not a pre-existing but undiscovered algorithm.

277.   The '941 patent claims require the use of a computer system.

278.   The '941 patent claims systems and methods not merely for transferring secure information over a computer network, but for making the computer network itself more secure.

279.   The claimed invention in the '941 claims is rooted in computer technology and overcomes problems specifically arising in the realm of computer networks.

---

[75] Nary Subramanian, *Biometric Authentication*, in ENCYCLOPEDIA OF CRYPTOGRAPHY AND SECURITY (S. Jajodia and H.C.A. van Tilborg 2nd ed. 2011) ("Biometric authentication is a technique for identifying the person accessing a secured asset . . . by comparing their unique biological features . . . [an] issue with biometric authentication is privacy of personal data.").

280.   The systems and methods claimed in the '941 patent were not a longstanding or fundamental economic practice at the time of patented inventions. Nor were they fundamental principles in ubiquitous use on the Internet or computers in general.

281.   The asserted claims do not involve a method of doing business that happens to be implemented on a computer; instead, it involves a method for changing digital records in a way that will affect the communication system itself, by making it more secure.

282.   One or more claims of the '941 patent require a specific configuration of electronic devices, a network configuration, and the use of encryption systems to secure communications and manage access to secure digital records. These are meaningful limitations that tie the claimed methods and systems to specific machines. For example, the below diagram from the '941 patent illustrates a specific configuration of hardware disclosed in the patent.
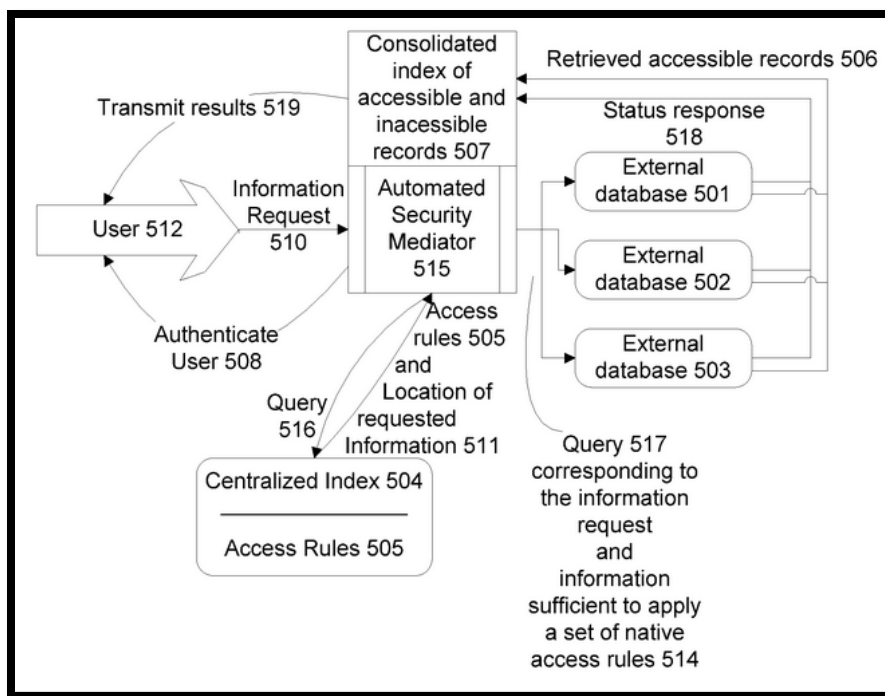
'941 patent, Fig. 6.

<div align="center">

COUNT I
INFRINGEMENT OF U.S. PATENT NO. 8,316,237

</div>

283.   St. Luke references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

284.   Apple makes, uses, sells, and/or offers for sale in the United States products and/or services for secure three-party communications.

285.   Apple makes, sells, offers to sell, imports, and/or uses Apple iMessage ("iMessage").

286.   Apple makes, sells, offers to sell, imports, and/or uses Apple FaceTime ("FaceTime").

287.   Apple makes, sells, offers to sell, imports, and/or uses Apple Handoff ("Handoff").

288.   Apple makes, sells, offers to sell, imports, and/or uses Apple iOS mobile devices (e.g., iPhone, iPad, iPod Touch) ("iOS")

289.   Apple builds and offers to its customers the applications, services, and devices: iMessage, FaceTime, Handoff, and iOS (collectively, the "Apple '237 Products").

290.   On information and belief, one or more of the Apple '237 Products include encryption technology.

291.   On information and belief, one or more of the Apple '237 Products enable sending encrypted information through an intermediary where the intermediary is not able to access the unencrypted message.

292.   On information and belief, the Apple '237 Products are available to businesses and individuals throughout the United States.

293.   On information and belief, the Apple '237 Products are provided to businesses and individuals located in the Eastern District of Texas.

294.   On information and belief, the Apple '237 Products include an automated communication port configured to receive a first message representing an encrypted communication associated with a first set of asymmetric keys (*e.g.,* a first set of RSA-1280 asymmetric keys), to receive a transcryption key (*e.g.,* a session-specific RSA and/or AES

transcryption key), and to transmit a second message representing the encrypted communication associated with a second set of asymmetric keys (e.g., a second set of RSA-1280 asymmetric keys).

295.   On information and belief, the below diagram shows the encryption system used by one or more of the Apple '237 Products.
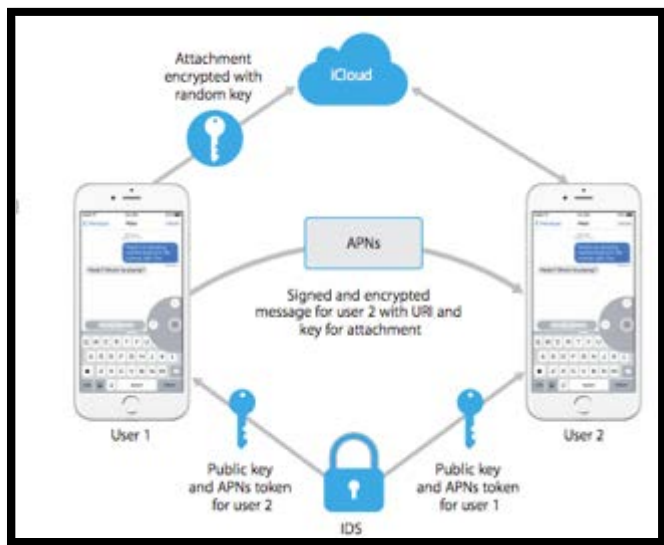
Source: iOS SECURITY – WHITE PAPER (June 2015).

296.   On information and belief, Apple iMessage server comprises an automated processor, configured to communicate through the automated communication port of and with the memory, to receive the first message, receive the transcryption key, automatically transcrypt the first message into the second message, and to transmit the second message.

297.   On information and belief, Apple FaceTime uses Internet Connectively Establishment (aka ICE) to establish a peer-to-peer connection between devices.

298.   On information and belief, Apple FaceTime verifies user identities through identity certificates and establishing a shared secret for each FaceTime session.

299.   On information and belief, Apple FaceTime uses cryptographic nonces supplied by each devices. The cryptographic nonces supplied by each device are combined to salt keys for each of the media channels, which are streamed via Secure Real Time Protocol (SRTP) using AES-256 encryption.

300.   On information and belief, iMessage generates two pairs of keys for use with the service – an RSA 1280-bit key for encryption and an ECDSA 256-bit key on the NIST P-256 curve (for signing).

301.   On information and belief, the iMessage server includes memory.

302.   Apple is the author of iOS Security – White Paper published in June 2015 available at: https://www.apple.com/business/docs/iOS_Security_Guide.pdf.

303.   On information and belief, Apple iMessage, FaceTime and Handoff can transmit information over a private network.

304.   On information and belief, one or more of the Apple '237 Products enable asymmetric encryption.

305.   On information and belief, Apple has directly infringed and continues to directly infringe the '237 patent by, among other things, making, using, offering for sale, and/or selling products and/or services for secure three-party communications, including but not limited to, the Apple '237 Products, which include infringing encryption technologies. Such products and/or services include, by way of example and without limitation, Apple iMessage, Apple FaceTime, Apple Handoff, and Apple iOS mobile devices (e.g., iPhone, iPad, iPod Touch).

306.   By making, using, testing, offering for sale, and/or selling encryption products and services, including but not limited to the Apple '237 Products, Apple has injured St. Luke and is liable to St. Luke for directly infringing one or more claims of the '237 patent, including at least claims 1, 2, 4, 5, 6, 8, 9, 12, 13, 15, and 17, pursuant to 35 U.S.C. § 271(a).

307.   On information and belief, Apple also infringes indirectly the '237 patent by active inducement under 35 U.S.C. § 271(b).

308.   Apple has had knowledge of the '237 patent since at least service of this Complaint or shortly thereafter, and on information and belief, Apple knew of the '237 patent and knew of its infringement, including by way of this lawsuit.

309.   On information and belief, Apple intended to induce patent infringement by third-party customers and users of the Apple '237 Products and had knowledge that the inducing acts

103

would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Apple specifically intended and was aware that the normal and customary use of the accused products would infringe the '237 patent. Apple performed the acts that constitute induced infringement, and would induce actual infringement, with the knowledge of the '237 patent and with the knowledge, that the induced acts would constitute infringement. For example, Apple provides the Apple '237 Products that have the capability of operating in a manner that infringe one or more of the claims of the '237 patent, including at least claims 1, 2, 4, 5, 6, 8, 9, 12, 13, 15, and 17, and Apple further provides documentation and training materials that cause customers and end users of the Apple '237 Products to utilize the products in a manner that directly infringe one or more claims of the '237 patent. By providing instruction and training to customers and end-users on how to use the Apple '237 Products in a manner that directly infringes one or more claims of the '237 patent, including at least claims 1, 2, 4, 5, 6, 8, 9, 12, 13, 15, and 17, Apple specifically intended to induce infringement of the '237 patent. On information and belief, Apple engaged in such inducement to promote the sales of the Apple '237 Products, *e.g.,* through Apple's user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '237 patent.[76] Accordingly, Apple has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '237 patent, knowing that such use constitutes infringement of the '237 patent.

310.   To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '237 patent.

311.   As a result of Apple's infringement of the '237 patent, St. Luke has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Apple's infringement, but in no event less than a reasonable royalty for the use made of the invention by Apple together with interest and costs as fixed by the Court.

---

[76] *See e.g.*, iOS Security Guide (June 2015),
https://www.apple.com/business/docs/iOS_Security_Guide.pdf.

COUNT II
INFRINGEMENT OF U.S. PATENT NO. 7,181,017

312.   St. Luke references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

313.   Apple makes, uses, sells, and/or offers for sale in the United States products and/or services for secure three-party communications.

314.   Apple makes, sells, offers to sell, imports, and/or uses Apple iMessage ("iMessage").

315.   Apple makes, sells, offers to sell, imports, and/or uses Apple HomeKit ("HomeKit").

316.   Apple makes, sells, offers to sell, imports, and/or uses Apple iCloud ("iCloud").

317.   Apple makes, sells, offers to sell, imports, and/or uses Apple iOS mobile devices (e.g., iPhone, iPad, iPod Touch) ("iOS").

318.   Apple builds and offers to its customers the applications, services, and devices: iMessage, HomeKit, iCloud, and iOS (collectively, the "Apple '017 Products").

319.   On information and belief, one or more of the Apple '017 Products include encryption technology.

320.   On information and belief, one or more of the Apple '017 Products enable sending encrypted information through an intermediary where the intermediary is not able to view the unencrypted message.

321.   On information and belief, the Apple '017 Products are available to businesses and individuals throughout the United States.

322.   On information and belief, the Apple '017 Products are provided to businesses and individuals located in the Eastern District of Texas.
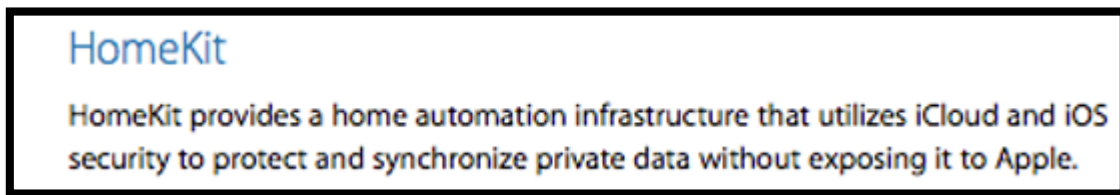
323.   On information and belief, Apple iMessage server receives information to be processed from a sending iOS mobile device.

324.   On information and belief, the HomeKit framework on an Apple iOS mobile device (e.g., iPhone, iPad, or iPod Touch) enables receiving information to be processed (e.g., HomeKit data).

325.   On information and belief, HomeKit identify and security are based on Ed25519 public-private key pairs.

326.   On information and belief, HomeKit provides a home automation infrastructure that utilizes iCloud and iOS security.

327.   Apple documentation represents HomeKit as enabling the synchronization of private data without exposing it to Apple.

HomeKit

HomeKit provides a home automation infrastructure that utilizes iCloud and iOS security to protect and synchronize private data without exposing it to Apple.

Source: iOS Security Guide 20 (June 2015),
https://www.apple.com/business/docs/iOS_Security_Guide.pdf.

328.   On information and belief, Apple iCloud server receives information (e.g., iCloud Drive, CloudKit, or iCloud Backup information) to be processed from a sending iOS mobile device (e.g., iPhone, iPad, or iPod Touch).

329.   On information and belief, Apple iCloud breaks each file into chunks and the file is encrypted using AES-128 and a key derived from each chunk's contents that utilizes SHA-256.

330.   On information and belief, iMessage defines a cryptographic comprehension function (e.g., session-specific cryptographic key, cipher suite, cryptographic mode of operation, initial conditions, and/or other cryptographic comprehension information) for the iMessage information, adapted for making at least a portion of the information incomprehensible.

331.   On information and belief, iMessage generates two key pairs for transmitting messages. The first key is an RSA 1280-bit key for encryption. The second key is an ECDSA 256-bit key on the NIST P-256 curve.

332.   On information and belief, iMessage uses private keys for both key pairs. The private keys are saved in a device's keychain and the public keys are sent to Apple's directory service.

333.   The below schematic shows the exchange of keys in iMessage for communication between two devices.
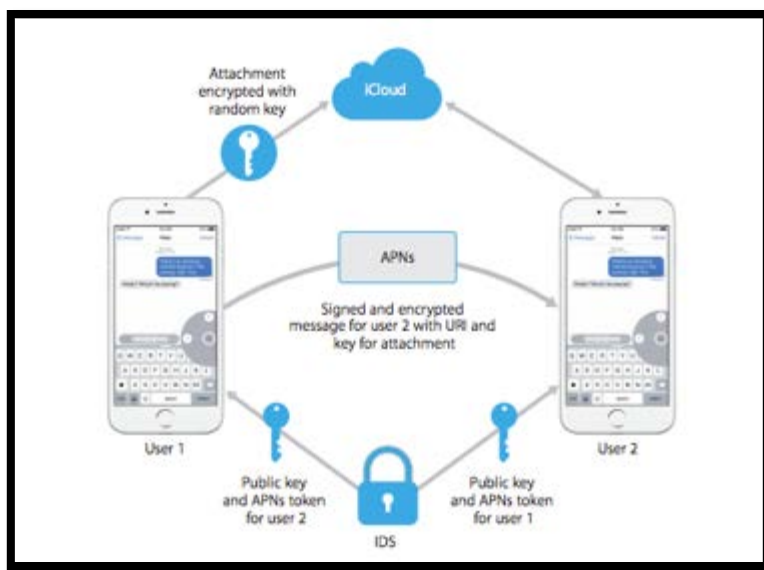
Source: iOS Security Guide 36 (June 2015),
https://www.apple.com/business/docs/iOS_Security_Guide.pdf.

334.   On information and belief, HomeKit defines a cryptographic comprehension function (e.g., session-specific cryptographic key, cipher suite, cryptographic mode of operation, initial conditions, and/or other cryptographic comprehension information) for the information (e.g., HomeKit home data), adapted for making at least a portion of the information incomprehensible.

335.   On information and belief, iCloud defines a cryptographic comprehension function (e.g., session-specific cryptographic key, cipher suite, cryptographic mode of operation, initial conditions, and/or other cryptographic comprehension information) for the information (e.g., iCloud Drive, CloudKit, or iCloud Backup information), adapted for making at least a portion of the information incomprehensible.

336.   On information and belief, the Apple '017 Products use "end-to-end" encryption.

107

337.   On information and belief, Apple iMessage server receives asymmetric key information (e.g., device-specific RSA-1280 asymmetric key information), comprising at least asymmetric encryption key information and asymmetric decryption key information.

338.   On information and belief, Apple HomeKit framework receives asymmetric key information (e.g., device- and/or user-specific Ed25519 asymmetric key information), comprising at least asymmetric encryption key information and asymmetric decryption key information.

339.   On information and belief, iCloud server receives asymmetric key information (e.g., device-and/or user-specific Curve25519 asymmetric key information), comprising at least asymmetric encryption key information, and asymmetric decryption key information.

340.   On information and belief, iMessage negotiates a new cryptographic comprehension function (e.g., new session-specific cryptographic key, cipher suite, cryptographic mode of operation, initial conditions, and/or other cryptographic comprehension information) between two parties to an iMessage communication (e.g., sending and receiving iOS mobile devices) using an iMessage server intermediary.

341.   On information and belief, HomeKit negotiates a new cryptographic comprehension function (e.g., new session-specific cryptographic key, cipher suite, cryptographic mode of operation, initial conditions, and/or other cryptographic comprehension information) between two parties to a HomeKit communication (e.g., sending and receiving iOS mobile devices and/or HomeKit-registered accessories) using a HomeKit framework intermediary.

342.   On information and belief, iCloud negotiates a new cryptographic comprehension function (e.g., new session-specific cryptographic key, cipher suite, cryptographic mode of operation, initial conditions, and/or other cryptographic comprehension information) between two parties to an iCloud communication (e.g., sending iOS mobile device and receiving third-party cloud storage server and/or mobile device) using an iCloud server intermediary.

343.   On information and belief, iMessage processes the information to invert the cryptographic comprehension function (e.g., the initial session-specific iMessage cryptographic key, cipher suite, cryptographic mode of operation, initial conditions, and/or other cryptographic comprehension information) and impose the new cryptographic comprehension function (e.g., the new session-specific iMessage cryptographic key, cipher suite, cryptographic mode of operation, initial conditions, and/or other cryptographic comprehension information) in an integral process, in dependence on at least the asymmetric cryptographic key information (e.g., the device-specific RSA-1280 asymmetric key information), without providing the intermediary (e.g., the iMessage server intermediary) with sufficient asymmetric key information to decrypt the processed information.

344.   On information and belief, HomeKit processes the information to invert the cryptographic comprehension function (e.g., the initial session-specific HomeKit cryptographic key, cipher suite, cryptographic mode of operation, initial conditions, and/or other cryptographic comprehension information) and impose the new cryptographic comprehension function (e.g., the new session-specific HomeKit cryptographic key, cipher suite, cryptographic mode of operation, initial conditions, and/or other cryptographic comprehension information) in an integral process, in dependence on at least the asymmetric cryptographic key information (e.g., the user and/or device-specific Ed25519 asymmetric key information), without providing the intermediary (e.g., the HomeKit framework intermediary) with sufficient asymmetric key information to decrypt the processed information.

345.   On information and belief, iCloud processes the information to invert the cryptographic comprehension function (e.g., the initial session-specific iCloud cryptographic key, cipher suite, cryptographic mode of operation, initial conditions, and/or other cryptographic comprehension information) and impose the new cryptographic comprehension function (e.g., the new session-specific iCloud cryptographic key, cipher suite, cryptographic mode of operation, initial conditions, and/or other cryptographic comprehension information) in an integral process, in dependence on at least the asymmetric cryptographic key information (e.g.,

the user and/or device-specific Curve25519 asymmetric key information), without providing the intermediary (e.g., the iCloud server intermediary) with sufficient asymmetric key information to decrypt the processed information.

346.   On information and belief, HomeKit framework outputs processed information (e.g., HomeKit data) for receipt by one or more iOS mobile devices and/or HomeKit-registered accessories.

347.   On information and belief, Apple iCloud server outputs processed information (e.g., processed iCloud Drive, CloudKit, or iCloud Backup information) for receipt by a receiving third-party cloud storage server (e.g., Amazon S3 or Microsoft Azure) and/or one or more receiving iOS mobile devices (e.g., iPhone, iPad, and/or iPod Touch).

348.   On information and belief, the asymmetric decryption key information (e.g., the device-specific iMessage RSA-1280 private key information) to decrypt the processed information (e.g., the processed iMessage information) changes dynamically (e.g., as iMessage cryptographic comprehension function information is renegotiated between the iMessage server and the iOS device sender/recipient(s)).

349.   On information and belief, the ability of the asymmetric decryption key information (e.g., the device- and/or user-specific Ed25519 private key information) to decrypt the processed information (e.g., the HomeKit information) changes dynamically (e.g., as HomeKit cryptographic comprehension function information is [re-]negotiated between/among the iOS device sender/recipient[s] and registered HomeKit accessories).

350.   On information and belief, ability of the asymmetric decryption key information (e.g., the device and/or user-specific Curve25519 asymmetric decryption key information) to decrypt the processed information (e.g., the processed iCloud Drive, CloudKit, or iCloud Backup information) changes dynamically (e.g., as iCloud cryptographic comprehension function information is renegotiated between/among the iOS device sender/recipient(s) and registered iCloud accessories).

351.   On information and belief, Apple has directly infringed and continues to directly infringe the '017 patent by, among other things, making, using, offering for sale, and/or selling products and/or services for secure three-party communications, including but not limited to, the Apple '017 Products, which include infringing encryption technologies. Such products and/or services include, by way of example and without limitation, Apple iMessage, Apple HomeKit, Apple iCloud, Apple iOS mobile devices (e.g., iPhone, iPad, iPod Touch).

352.   By making, using, testing, offering for sale, and/or selling encryption products and services, including but not limited to the Apple '017 Products, Apple has injured St. Luke and is liable to St. Luke for directly infringing one or more claims of the '017 patent, including at least claim 1, pursuant to 35 U.S.C. § 271(a).

353.   On information and belief, Apple also infringes indirectly the '017 patent by active inducement under 35 U.S.C. § 271(b).

354.   On information and belief, Apple had knowledge of the '017 patent since at least 2002. Apple cited the '017 patent in the following issued United States Patents:

- U.S. Patent No. 7,587,047 issued on September 8, 2009 and assigned to Apple.
- U.S. Patent No. 7,650,507 issued on January 19, 2010 and assigned to Apple.
- U.S. Patent No. 8,064,888 issued on November 22, 2011 and assigned to Apple.
- U.S. Patent No. 8,320,889 issued on November 27, 2012 and assigned to Apple.
- U.S. Patent No. 8,402,273 issued on March 19, 2013 and assigned to Apple.
- U.S. Patent No. 8,412,164 issued on April 2, 2013 and assigned to Apple.
- U.S. Patent No. 8,555,067 issued on October 8, 2013 and assigned to Apple.
- U.S. Patent No. 8,681,975 issued on March 25, 2014 and assigned to Apple.
- U.S. Patent No. 9,106,447 issued on August 11, 2015 and assigned to Apple.
- U.S. Patent Application No. 2011/0051931 published March 3, 2011 and assigned to Apple.

355.   Alternatively, on information and belief, Apple has had knowledge of the '017 patent since at least service of this Complaint or shortly thereafter, and on information and belief, Apple knew of the '017 patent and knew of its infringement, including by way of this lawsuit.

356.   On information and belief, Apple intended to induce patent infringement by third-party customers and users of the Apple '017 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Apple specifically intended and was aware that the normal and customary use of the accused products would infringe the '017 patent. Apple performed the acts that constitute induced infringement, and would induce actual infringement, with the knowledge of the '017 patent and with the knowledge, that the induced acts would constitute infringement. For example, Apple provides the Apple '017 Products that have the capability of operating in a manner that infringe one or more of the claims of the '017 patent, including at least claim 1, and Apple further provides documentation and training materials that cause customers and end users of the Apple '017 Products to utilize the products in a manner that directly infringe one or more claims of the '017 patent. By providing instruction and training to customers and end-users on how to use the Apple '017 Products in a manner that directly infringes one or more claims of the '017 patent, including at least claim 1, Apple specifically intended to induce infringement of the '017 patent. On information and belief, Apple engaged in such inducement to promote the sales of the Apple '017 Products, *e.g.,* through Apple's user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '017 patent.[77] Accordingly, Apple has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '017 patent, knowing that such use constitutes infringement of the '017 patent.

357.   To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '017 patent.

---

[77] *See e.g.*, iOS Security Guide (June 2015),
https://www.apple.com/business/docs/iOS_Security_Guide.pdf

358.   As a result of Apple's infringement of the '017 patent, St. Luke has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Apple's infringement, but in no event less than a reasonable royalty for the use made of the invention by Apple together with interest and costs as fixed by the Court.

<div align="center">

COUNT III
INFRINGEMENT OF U.S. PATENT NO. 7,869,591

</div>

359.   St. Luke references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

360.   Apple makes, uses, sells, and/or offers for sale in the United States products and/or services for secure three-party communications.

361.   Apple makes, sells, offers to sell, imports, and/or uses Apple iMessage ("iMessage").

362.   Apple makes, sells, offers to sell, imports, and/or uses Apple FaceTime ("FaceTime").

363.   Apple makes, sells, offers to sell, imports, and/or uses Apple Handoff ("Handoff").

364.   Apple makes, sells, offers to sell, imports, and/or uses Apple iOS mobile devices (e.g., iPhone, iPad, iPod Touch).

365.   Apple builds and offers to its customers the applications, services, and devices: iMessage, FaceTime, and Handoff, iOS (collectively, the "Apple '591 Products").

366.   On information and belief, one or more of the Apple '591 Products include encryption technology.

367.   On information and belief, one or more of the Apple '591 Products enable sending encrypted information through an intermediary where the intermediary is not able to view the unencrypted message.

368.   On information and belief, the Apple '591 Products are available to businesses and individuals throughout the United States.

369.   On information and belief, the Apple '591 Products are provided to businesses and individuals located in the Eastern District of Texas.

370.   On information and belief, an Apple iMessage server receives and stores in a first memory information encrypted based on a first set of cryptographic keys (e.g., a first set of RSA-1280 asymmetric keys), a first portion (e.g., a private key portion) of the first set of cryptographic keys having been employed to produce the encrypted information and a second portion (e.g., a public key portion) of the first set of cryptographic keys being required to decrypt the information encrypted with the first portion of the first set of cryptographic information (e.g., the first set of RSA-1280 asymmetric keys).

371.   The below schematic shows the exchange of keys in iMessage for communication between two devices.
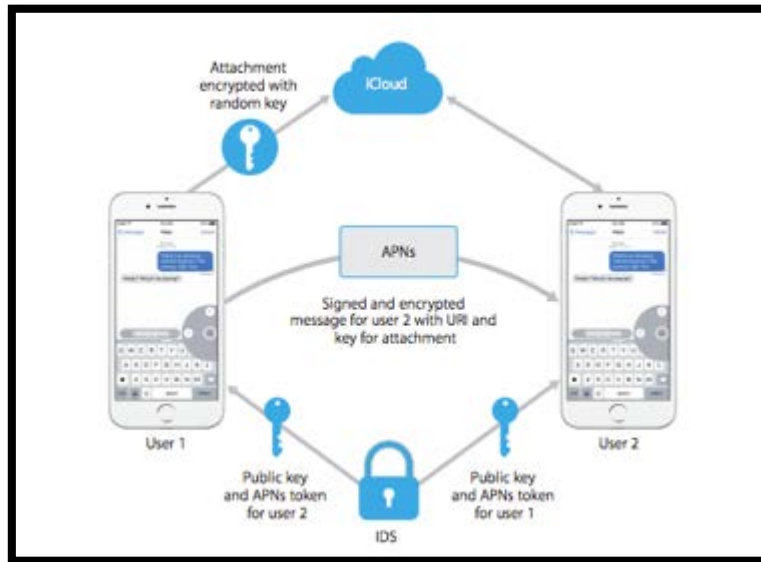
Source: iOS Security Guide 36 (June 2015),
https://www.apple.com/business/docs/iOS_Security_Guide.pdf.

372.   On information and belief, an Apple iMessage server receives and stores in a second memory (e.g., privileged memory dedicated to cryptographic key storage and/or manipulation) a first portion (e.g., a public key portion) of a second set of cryptographic keys (e.g., a second set of RSA-1280 asymmetric keys), having a corresponding second portion (e.g., a private key portion) being required for decryption of a message encrypted using the first

portion of the second set of cryptographic keys (e.g., the public key portion of the second set of RSA-1280 asymmetric keys).

373.   On information and belief, Apple iMessage transcryption is representative of at least Apple FaceTime and Apple Handoff transcryption. *See, e.g.,* iOS Security – White Paper (June 2015) at 36, 42-44.

374.   On information belief, an Apple iMessage server negotiates a set of session keys (e.g., RSA and/or AES session keys) through a communications port.

375.   On information and belief, an iMessage server without requiring or employing sufficient information either to decrypt the encrypted information or to comprehend the transcrypted information generates a transcryption key for transforming the received encrypted information to transcrypted information.

376.   On information and belief, an iMessage server without requiring or employing sufficient information either to decrypt the encrypted information or to comprehend the transcrypted information, transcrypts the stored encrypted information into transcrypted information using the transcryption key.

377.   On information and belief, an iMessage server generates a transcryption key for transforming the received encrypted information to transcrypted information, in dependence on at least information representing the second portion of the first set of cryptographic keys (e.g., information representing the public key portion of the first set of RSA-1280 asymmetric cryptographic keys), information representing the first portion of the second set of cryptographic keys (e.g., information representing the public key portion of the second set of RSA-1280 asymmetric cryptographic keys), and a first portion of the set of session keys (e.g., a first portion of the set of RSA and/or AES session keys).

378.   On information and belief, the Apple '591 Products transcrypt information wherein at least one of the first set of cryptographic keys, the second set of cryptographic keys, and the set of session keys, are key pairs related through at least one cryptographic algorithm selected from the group consisting of one or more of an elliptic curve cryptographic algorithm, a

Rivest-Shamir-Adleman cryptographic algorithm, an El Gamal cryptographic algorithm,[78] and a Diffie-Hellman cryptographic algorithm.

379.   On information and belief, iMessage transcrypts information wherein at least one of the first set of iMessage cryptographic keys, the second set of iMessage cryptographic keys, and the set of iMessage session keys, are key pairs related through at least one of an elliptic curve cryptographic algorithm, an RSA cryptographic algorithm, and a Diffie-Hellman cryptographic algorithm.

380.   On information and belief, the Apple '591 Products transcrypt information by authenticating a remote system and communicating the transcryption key to the authenticated remote system.

381.   On information and belief, an Apple iMessage transcrypts information by authenticating a remote system and communicating the transcryption key to the authenticated remote system at least where the transcryption key is generated on an Apple iMessage server remote from the server where the transcryption key is to be deployed.

382.   On information and belief, the Apple '591 Products transcrypt information wherein the first set of cryptographic keys is associated with a first party, the second set of cryptographic keys is associated with a second party, and the method is conducted without exchanging cryptographic information between the first party and second party sufficient for decrypting the encrypted information or comprehending the transcrypted information.

383.   On information and belief, Apple iMessage transcrypts information wherein the first set of cryptographic keys (e.g., the first set of RSA-1280 asymmetric keys) is associated with a first party (e.g., an iMessage sender), the second set of cryptographic keys (e.g., the second set of RSA-1280 asymmetric keys) is associated with a second party (e.g., an iMessage recipient), and Apple's iMessage service does not exchange cryptographic information between

---

[78] *See* Yvo Desmedt, *ElGamal Public Key Encryption*, ENCYCLOPEDIA OF CRYPTOGRAPHY AND SECURITY at 396 (2011) ("[t]he ElGamal public key encryption scheme is characterized by having as ciphertext, $(c1,c2):=(g^k, m \cdot y^k_A)$").

the first party and second party sufficient for decrypting the encrypted information or comprehending the transcrypted information.

384.   On information and belief, Apple '591 Products transcrypt information where the set of session keys is dynamically generated for use in conjunction with a communication session, and the transcryption key and the second set of cryptographic keys together provide insufficient information to determine key components of the first set of cryptographic keys.

385.   On information and belief, Apple iMessage transcrypts information wherein the set of iMessage session keys is dynamically generated for use in conjunction with an iMessage communication session, and the transcryption key and the second set of cryptographic keys together provide insufficient information to determine key components of the first set of cryptographic keys.

386.   On information and belief, Apple '591 Products transcrypt information wherein the session keys are negotiated through the communication port with an intended recipient of the transcrypted information.

387.   On information and belief, iMessage session keys are negotiated through a communication port with an intended recipient of the transcrypted information.

388.   On information and belief, Apple has directly infringed and continues to directly infringe the '591 patent by, among other things, making, using, offering for sale, and/or selling products and/or services for secure three-party communications, including but not limited to, the Apple '591 Products, which include infringing encryption technologies. Such products and/or services include, by way of example and without limitation, Apple iMessage, Apple FaceTime, Apple Handoff, and Apple iOS mobile devices (e.g., iPhone, iPad, iPod Touch).

389.   By making, using, testing, offering for sale, and/or selling encryption products and services, including but not limited to the Apple '591 Products, Apple has injured St. Luke and is liable to St. Luke for directly infringing one or more claims of the '591 patent, including at least claims 13, 14, 15, 16, 18, 20, and 21, pursuant to 35 U.S.C. § 271(a).

390.   On information and belief, Apple also infringes indirectly the '591 patent by active inducement under 35 U.S.C. § 271(b).

391.   Apple has had knowledge of the '591 patent since at least service of this Complaint or shortly thereafter, and on information and belief, Apple knew of the '591 patent and knew of its infringement, including by way of this lawsuit.

392.   On information and belief, Apple intended to induce patent infringement by third-party customers and users of the Apple '591 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Apple specifically intended and was aware that the normal and customary use of the accused products would infringe the '591 patent. Apple performed the acts that constitute induced infringement, and would induce actual infringement, with the knowledge of the '591 patent and with the knowledge, that the induced acts would constitute infringement. For example, Apple provides the Apple '591 Products that have the capability of operating in a manner that infringe one or more of the claims of the '591 patent, including at least claims 13, 14, 15, 16, 18, 20, and 21, and Apple further provides documentation and training materials that cause customers and end users of the Apple '591 Products to utilize the products in a manner that directly infringe one or more claims of the '591 patent. By providing instruction and training to customers and end-users on how to use the Apple '591 Products in a manner that directly infringes one or more claims of the '591 patent, including at least claims 13, 14, 15, 16, 18, 20, and 21, Apple specifically intended to induce infringement of the '591 patent. On information and belief, Apple engaged in such inducement to promote the sales of the Apple '591 Products, *e.g.,* through Apple's user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '591 patent.[79] Accordingly, Apple has induced and continues to induce users of the accused products to use the accused

---

[79] *See e.g.*, iOS Security Guide (June 2015),
https://www.apple.com/business/docs/iOS_Security_Guide.pdf.

products in their ordinary and customary way to infringe the '591 patent, knowing that such use constitutes infringement of the '591 patent.

393.   To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '591 patent.

394.   As a result of Apple's infringement of the '591 patent, St. Luke has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Apple's infringement, but in no event less than a reasonable royalty for the use made of the invention by Apple together with interest and costs as fixed by the Court.

<div align="center">

COUNT IV
INFRINGEMENT OF U.S. PATENT NO. 8,904,181

</div>

395.   St. Luke references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

396.   Apple makes, uses, sells, and/or offers for sale in the United States products and/or services for secure three-party communications.

397.   Apple makes, sells, offers to sell, imports, and/or uses Apple iMessage ("iMessage").

398.   Apple makes, sells, offers to sell, imports, and/or uses Apple FaceTime ("FaceTime").

399.   Apple makes, sells, offers to sell, imports, and/or uses Apple Handoff ("Handoff").

400.   Apple makes, sells, offers to sell, imports, and/or uses Apple iOS mobile devices (e.g., iPhone, iPad, iPod Touch) ("iOS").

401.   Apple builds and offers to its customers the applications, services, and devices: iMessage, FaceTime, Handoff, and iOS (collectively, the "Apple '181 Products").

402.   On information and belief, one or more of the Apple '181 Products include encryption technology.

403.   On information and belief, one or more of the Apple '181 Products enable sending encrypted information through an intermediary where the intermediary is not able to view the unencrypted message.

404.   On information and belief, the Apple '181 Products are available to businesses and individuals throughout the United States.
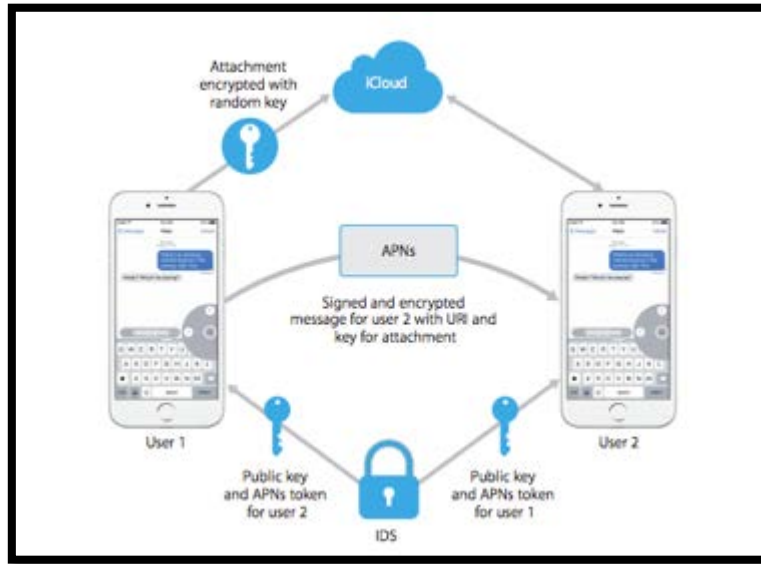
405.   On information and belief, the Apple '181 Products are provided to businesses and individuals located in the Eastern District of Texas.

406.   On information and belief, the Apple '181 Products use at least one key handler (e.g., an iMessage, FaceTime, and/or Handoff key handler) comprising an interface to a memory which stores a plurality of encrypted records, each encrypted record having an associated asymmetric encryption key pair and being encrypted with a first component of the associated asymmetric encryption key pair.

407.   On information and belief, an Apple iMessage key handler is representative of at least an Apple FaceTime key handler and an Apple Handoff key handler with respect to at least one charted mechanism of infringement of this claim limitation.

408.   On information and belief, an Apple iMessage key handler comprises an interface to a memory which stores a plurality of encrypted records (e.g., encrypted iMessage records), each encrypted record having an associated asymmetric encryption key pair (e.g., an associated RSA-1280 asymmetric key pair) and being encrypted with a first component (e.g., a private key component) of the associated asymmetric encryption key pair.

409.   The below schematic shows the exchange of keys in iMessage for communication between two devices.

Source: iOS Security Guide 36 (June 2015),
https://www.apple.com/business/docs/iOS_Security_Guide.pdf.

410.   On information and belief, the Apple '181 Products use at least one key handler
(e.g., an iMessage, FaceTime, and/or Handoff key handler) comprising at least one automated
processor operating in a privileged processing environment, configured to receive a selected
encrypted record from the memory through the interface, to negotiate at least one asymmetric
session key, and to transcrypt the encrypted message to a transcrypted message in an integral
process substantially without intermediate decryption, using a transcryption key derived at least
in part from the at least one asymmetric session key.

411.   On information and belief, an Apple iMessage key handler comprises at least one
automated processor operating in a privileged processing environment (e.g., a privileged Intel
TXT processing environment or similar privileged server execution environment), configured to
receive a selected encrypted record (e.g., a selected encrypted iMessage record) from the
memory through the interface, to negotiate at least one asymmetric session key (e.g., at least one
RSA-OAEP asymmetric session key), and to transcrypt the encrypted message to a transcrypted
message in an integral process substantially without intermediate decryption, using a
transcryption key derived at least in part from the at least one asymmetric session key.

412.   On information and belief, the Apple '181 Products use at least one key handler (e.g., an iMessage, FaceTime, and/or Handoff key handler) comprising a communication port configured to conduct the negotiation for the at least one asymmetric session key and to communicate the transcrypted record.

413.   On information and belief, Apple iMessage transcryption is representative of at least Apple FaceTime and Apple Handoff transcryption with respect to the claims of the '181 patent. *See, e.g.,* iOS Security – White Paper (June 2015) at 36, 42-44.

414.   On information and belief, the Apple '181 Products' key handler is configured to communicate with the memory through a virtual private network.

415.   On information and belief, the Apple '181 Products' key handler is enabled to use an associated asymmetric key pair comprising a Diffie-Hellman type key.

416.   On information and belief, the Apple '181 Products' key handler is enabled to use an associated asymmetric key pair comprising a Rivest-Shamir-Adler type key.

417.   On information and belief, the Apple '181 Products' key handler is enabled to use an associated asymmetric key pair comprising at least one of an elliptic curve key pair and an ElGamal key pair.

418.   On information and belief, an Apple iMessage key handler comprises at least one communication port configured to conduct the negotiation for the at least one asymmetric session key (e.g., the negotiation for the at least one RSA-OAEP asymmetric session key) and to communicate the transcrypted record (e.g., the transcrypted iMessage record).

419.   On information and belief, the Apple '181 Products use a transcryption key that has as components at least a second asymmetric component of the associated asymmetric key pair, and the at least one asymmetric session key, to result in a transcrypted message encrypted with at least one asymmetric session key.

420.   On information and belief, the Apple '181 Products' key handler wherein at least one asymmetric session key comprises at least two asymmetric session keys negotiated with at

least two respectively different parties, at least one of the two respectively different parties being a non-recipient of the transcrypted record.

421.   On information and belief, the Apple '181 Products' key handler uses a transcryption key that has as components at least a second component of the associated asymmetric encryption key pair, the at least one asymmetric session key, and a received asymmetric key component, to result in a transcrypted message encrypted with at least one asymmetric session key and the received asymmetric key component.

422.   On information and belief, an Apple iMessage server stores, in at least one database, a plurality of encrypted records (e.g., encrypted iMessage records), each encrypted record having an associated asymmetric encryption key pair (e.g., an associated RSA-1280 asymmetric key pair) and being encrypted with a first component (e.g., a private key component) of the associated asymmetric encryption key pair.

423.   On information and belief, an Apple iMessage server negotiates, by the automated key handler, at least one asymmetric session key (e.g., at least one RSA-OAEP asymmetric session key).

424.   On information and belief, the Apple '181 Products store encrypted records, each encrypted record having an associated asymmetric encryption key pair and being encrypted with a first component of the associated asymmetric encryption key pair, in a database.

425.   On information and belief, an Apple iMessage server receives an encrypted message (e.g., an encrypted iMessage record) by an automated key handler operating in a privileged processing environment (e.g., a privileged Intel TXT processing environment or similar privileged server execution environment), through an interface (e.g., a server-client (e.g., iDevice) network interface).

426.   On information and belief, an Apple iMessage server transcrypts, by the automated key handler, the encrypted message (e.g., the encrypted iMessage message) to a transcrypted message in an integral process substantially without intermediate decryption, using a transcryption key.

123

427.   On information and belief, Apple has directly infringed and continues to directly infringe the '181 patent by, among other things, making, using, offering for sale, and/or selling products and/or services for secure three-party communications, including but not limited to, the Apple181 Products, which include infringing encryption technologies. Such products and/or services include, by way of example and without limitation, Apple iMessage, Apple FaceTime, Apple Handoff, and Apple iOS mobile devices (e.g., iPhone, iPad, iPod Touch).

428.   By making, using, testing, offering for sale, and/or selling encryption products and services, including but not limited to the Apple '181 Products, Apple has injured St. Luke and is liable to St. Luke for directly infringing one or more claims of the '181 patent, including at least claims 1-4 and 6-17, pursuant to 35 U.S.C. § 271(a).

429.   On information and belief, Apple also infringes indirectly the '181 patent by active inducement under 35 U.S.C. § 271(b).

430.   Apple has had knowledge of the '181 patent since at least service of this Complaint or shortly thereafter, and on information and belief, Apple knew of the '181 patent and knew of its infringement, including by way of this lawsuit.

431.   On information and belief, Apple intended to induce patent infringement by third-party customers and users of the Apple '181 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Apple specifically intended and was aware that the normal and customary use of the accused products would infringe the '181 patent. Apple performed the acts that constitute induced infringement, and would induce actual infringement, with the knowledge of the '181 patent and with the knowledge, that the induced acts would constitute infringement. For example, Apple provides the Apple '181 Products that have the capability of operating in a manner that infringe one or more of the claims of the '181 patent, including at least claims 1-4 and 6-17, and Apple further provides documentation and training materials that cause customers and end users of the Apple '181 Products to utilize the products in a manner that directly infringe one or more claims of the '181 patent. By providing instruction and training to customers and

end-users on how to use the Apple '181 Products in a manner that directly infringes one or more claims of the '181 patent, including at least claims 1-4 and 6-17, Apple specifically intended to induce infringement of the '181 patent. On information and belief, Apple engaged in such inducement to promote the sales of the Apple '181 Products, *e.g.,* through Apple's user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '181 patent.[80] Accordingly, Apple has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '181 patent, knowing that such use constitutes infringement of the '181 patent.

432. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '181 patent.

433. As a result of Apple's infringement of the '181 patent, St. Luke has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Apple's infringement, but in no event less than a reasonable royalty for the use made of the invention by Apple together with interest and costs as fixed by the Court.

COUNT V
INFRINGEMENT OF U.S. PATENT NO. 8,566,247

434. St. Luke references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

435. Apple makes, uses, sells, and/or offers for sale in the United States products and/or services for secure three-party communications.

436. Apple makes, sells, offers to sell, imports, and/or uses Apple iMessage ("iMessage").

437. Apple makes, sells, offers to sell, imports, and/or uses Apple FaceTime ("FaceTime").

---

[80] *See e.g.*, iOS Security Guide (June 2015), https://www.apple.com/business/docs/iOS_Security_Guide.pdf.

438.   Apple makes, sells, offers to sell, imports, and/or uses Apple Handoff ("Handoff").

439.   Apple makes, sells, offers to sell, imports, and/or uses iOS mobile devices (e.g., iPhone, iPad, iPod Touch) ("iOS").

440.   Apple builds and offers to its customers the applications, services, and devices: iMessage, FaceTime, Handoff, and iOS (collectively, the "Apple '247 Products").

441.   On information and belief, one or more of the Apple '247 Products include encryption technology.

442.   On information and belief, one or more of the Apple '247 Products enable sending encrypted information through an intermediary where the intermediary is not able to view the unencrypted message.

443.   On information and belief, the Apple '247 Products are available to businesses and individuals throughout the United States.

444.   On information and belief, the Apple '247 Products are provided to businesses and individuals located in the Eastern District of Texas.

445.   On information and belief, the Apple '247 Products include functionality for communicating information, which is encrypted from a first party to a second party, involving an intermediary that selectively authorizes the second party to comprehend the information, without the intermediary itself being enabled to comprehend the information, as claimed.

446.   On information and belief, an Apple server (e.g., an Apple iMessage, FaceTime, and/or Handoff server) communicates information (e.g., iMessage, FaceTime, and/or Handoff information) which is encrypted from a first party (e.g., an iMessage, FaceTime, and/or Handoff sender) to a second party (e.g., an iMessage, FaceTime and/or Handoff receiver). The communication involves an Apple-controlled intermediary (e.g., an iMessage, FaceTime, and/or Handoff intermediary) that selectively authorizes the second party (e.g., the iMessage, FaceTime, and/or Handoff sender) to comprehend the information without the Apple-controlled intermediary itself being enabled to comprehend the information.

126

447.   On information and belief, an Apple '247 Products' server identifies information to be communicated, the information being encrypted with an associated cryptographic comprehension function.

448.   On information and belief, the Apple iMessage server creates a cryptographic audit trail.

449.   On information and belief, the Apple '247 Products create a cryptographic audit trail.

450   On information and belief, an Apple iMessage key handler is representative of at least an Apple FaceTime key handler and an Apple Handoff key handler with respect to the claims in the '247 patent. *See, e.g.,* iOS Security – White Paper (June 2015) at 36, 42-44.

451.   On information and belief, Apple iMessage transcryption is representative of at least Apple FaceTime and Apple Handoff transcryption with respect to the claims in the '247 patent. *See, e.g.,* iOS Security – White Paper (June 2015) at 36, 42-44.

452.   On information and belief, an Apple iMessage server identifies information to be communicated (e.g., encrypted iMessage, FaceTime, and/or Handoff information received at the server from a first iDevice, the information to be communicated to a second iDevice), the information.

453.   On information and belief, an Apple iMessage server comprises at least one automated processor which conducts a negotiation between the second party (e.g., the iMessage, FaceTime, and/or Handoff receiving party) and the intermediary (e.g., the Apple-controlled iMessage, FaceTime, and/or Handoff intermediary) of an asymmetric delivery comprehension function (e.g., a receiver-side RSA and/or elliptical curve asymmetric comprehension function) of the information which is encrypted (e.g., the iMessage, FaceTime, and/or Handoff information that is encrypted).

454.   On information and belief, an asymmetric delivery comprehension function (e.g., the receiver-side RSA and/or elliptical curve asymmetric comprehension function) is different from the associated cryptographic comprehension function (e.g., the sender-side cryptographic

127

comprehension function). The asymmetric delivery comprehension function comprises a function of at least three asymmetric key components of at least three distinct respective asymmetric delivery comprehension functions (e.g., an iMessage sender-specific asymmetric key component of a first asymmetric delivery comprehension function; an Apple-controlled intermediary-specific asymmetric key component of a second asymmetric delivery comprehension function; and an iMessage receiver-specific asymmetric key component of a third asymmetric delivery comprehension function).

455.   On information and belief, the iMessage receiving party (second party) possesses an ability to decrypt the information (e.g., the iMessage, FaceTime, and/or Handoff information) which is encrypted with the asymmetric delivery comprehension function (e.g., the receiver-side RSA and/or elliptical curve asymmetric comprehension function), and the intermediary (e.g., the Apple-controlled iMessage intermediary) possesses a portion of the asymmetric delivery comprehension function which does not impart an ability to decrypt the information which is encrypted.

456.   On information and belief, an Apple iMessage server automated processor transforms a comprehension function of the information (e.g., iMessage, FaceTime, and/or Handoff) information which is encrypted to be communicated from the associated cryptographic comprehension function (e.g., the sender-side cryptographic comprehension function) to the asymmetric delivery cryptographic comprehension function (e.g., the receiver-side RSA and/or elliptical curve asymmetric comprehension function). The transformation comprises using the negotiated asymmetric delivery comprehension function of the at least three asymmetric key components of the at least three distinct respective asymmetric delivery comprehension functions (e.g., the iMessage sender-specific asymmetric key component of a first asymmetric delivery comprehension function; the Apple-controlled intermediary-specific asymmetric key component of a second asymmetric delivery comprehension function; and the iMessage receiver-specific asymmetric key component of a third asymmetric delivery comprehension function) in an integral process which does not have as an intermediate state a decrypted representation of the

128

information and does not itself require at any time during the transformation, knowledge
sufficient for decrypting the information which is encrypted.

457.   On information and belief, the Apple iMessage server communicates the
information (e.g., the iMessage, FaceTime, and/or Handoff information) which is encrypted with
the asymmetric delivery cryptographic comprehension function (e.g., the receiver-side RSA
and/or elliptical curve asymmetric comprehension function) to the second party (e.g., the
iMessage receiving party).

458.   On information and belief, the Apple '247 Products are systems for
communicating information (e.g., iMessage, FaceTime, and/or Handoff information) which is
encrypted from a first party (e.g., an iMessage, FaceTime, and/or Handoff sender) to a second
party (e.g., an iMessage, FaceTime and/or Handoff receiver). The systems involve an Apple-
controlled intermediary (e.g., an iMessage, FaceTime, and/or Handoff intermediary) that
selectively authorizes the second party (e.g., the iMessage, FaceTime, and/or Handoff sender) to
comprehend the information without the Apple-controlled intermediary itself being enabled to
comprehend the information.

459.   On information and belief, the Apple iMessage server comprises a
communication port (e.g., a server-iDevice client network communications port) which receives
information which is encrypted to be communicated (e.g., iMessage, FaceTime, and/or Handoff
information which is encrypted to be communicated) or an identification thereof, the information
being encrypted with an associated cryptographic comprehension function (e.g., a sender-side
cryptographic comprehension function).

460.   On information and belief, the Apple '247 Products include at least one
automated processor which conducts a negotiation between the second party and the
intermediary through the communication port of an asymmetric delivery comprehension function
of the information which is encrypted, different from the associated cryptographic
comprehension function, wherein the asymmetric delivery comprehension function comprises a
function of at least three asymmetric key components of at least three distinct respective

asymmetric delivery comprehension functions, wherein the second party possesses an ability to decrypt the information which is encrypted with the asymmetric delivery comprehension function, and the intermediary possesses a portion of the asymmetric delivery comprehension function which does not impart an ability to decrypt the information which is encrypted.

461.   On information and belief, the Apple iMessage server includes at least one automated processor which conducts a negotiation between the second party (e.g., the iMessage, FaceTime, and/or Handoff receiving party) and the intermediary (e.g., the Apple-controlled iMessage, FaceTime, and/or Handoff intermediary) through the communication port of an asymmetric delivery comprehension function (e.g., a receiver-side RSA and/or elliptical curve asymmetric comprehension function) of the information which is encrypted (e.g., the iMessage, FaceTime, and/or Handoff information that is encrypted).

462.   On information and belief, the Apple iMessage server's automated processor transforms a comprehension function of the information (e.g., iMessage, FaceTime, and/or Handoff) information which is encrypted to be communicated from the associated cryptographic comprehension function (e.g., the sender-side cryptographic comprehension function) to the asymmetric delivery cryptographic comprehension function (e.g., the receiver-side RSA and/or elliptical curve asymmetric comprehension function). The transformation comprises using the negotiated asymmetric delivery comprehension function of the at least three asymmetric key components of the at least three distinct respective asymmetric delivery comprehension functions (e.g., the iMessage sender-specific asymmetric key component of a first asymmetric delivery comprehension function; the Apple-controlled intermediary-specific asymmetric key component of a second asymmetric delivery comprehension function; and the iMessage receiver-specific asymmetric key component of a third asymmetric delivery comprehension function) in an integral process which does not have as an intermediate state a decrypted representation of the information and does not itself require at any time during the transformation, knowledge sufficient for decrypting the information which is encrypted.

463.   On information and belief, an Apple iMessage server communications port communicates the information (e.g., the iMessage, FaceTime, and/or Handoff information) which is encrypted with the asymmetric delivery cryptographic comprehension function (e.g., the receiver-side RSA and/or elliptical curve asymmetric comprehension function) to the second party (e.g., the iMessage receiving party).

464.   On information and belief, Apple has directly infringed and continues to directly infringe the '247 patent by, among other things, making, using, offering for sale, and/or selling products and/or services for secure three-party communications, including but not limited to, the Apple '247 Products, which include infringing encryption technologies. Such products and/or services include, by way of example and without limitation, Apple iMessage, Apple FaceTime, Apple Handoff, and Apple iOS mobile devices (*e.g*., iPhone, iPad, iPod Touch).

465.   By making, using, testing, offering for sale, and/or selling encryption products and services, including but not limited to the Apple '247 Products, Apple has injured St. Luke and is liable to St. Luke for directly infringing one or more claims of the '247 patent, including at least claims 1, 4, 7, 10, 13, 16, 19, and 20, pursuant to 35 U.S.C. § 271(a).

466.   On information and belief, Apple also infringes indirectly the '247 patent by active inducement under 35 U.S.C. § 271(b).

467.   Apple has had knowledge of the '247 patent since at least service of this Complaint or shortly thereafter, and on information and belief, Apple knew of the '247 patent and knew of its infringement, including by way of this lawsuit.

468.   On information and belief, Apple intended to induce patent infringement by third-party customers and users of the Apple '247 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Apple specifically intended and was aware that the normal and customary use of the accused products would infringe the '247 patent. Apple performed the acts that constitute induced infringement, and would induce actual infringement, with the knowledge of the '247 patent and with the knowledge, that the induced acts would constitute infringement. For

example, Apple provides the Apple '247 Products that have the capability of operating in a manner that infringe one or more of the claims of the '247 patent, including at least claims 1, 4, 7, 10, 13, 16, 19, and 20, and Apple further provides documentation and training materials that cause customers and end users of the Apple '247 Products to utilize the products in a manner that directly infringe one or more claims of the '247 patent. By providing instruction and training to customers and end-users on how to use the Apple '247 Products in a manner that directly infringes one or more claims of the '247 patent, including at least claims 1, 4, 7, 10, 13, 16, 19, and 20, and 17, Apple specifically intended to induce infringement of the '247 patent. On information and belief, Apple engaged in such inducement to promote the sales of the Apple '247 Products, *e.g.,* through Apple's user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '247 patent.[81] Accordingly, Apple has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '247 patent, knowing that such use constitutes infringement of the '247 patent.

469.   To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '247 patent.

470.   As a result of Apple's infringement of the '247 patent, St. Luke has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Apple's infringement, but in no event less than a reasonable royalty for the use made of the invention by Apple together with interest and costs as fixed by the Court.

COUNT VI
INFRINGEMENT OF U.S. PATENT NO. 7,587,368

471.   St. Luke references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

---

[81] *See e.g.*, iOS Security Guide (June 2015), https://www.apple.com/business/docs/iOS_Security_Guide.pdf

472.   Apple makes, sells, offers to sell, imports, and/or uses products and services that contain Apple FairPlay Streaming ("FairPlay Streaming").

473.   On information and belief, Apple released FairPlay Streaming to application and content developers in 2015.[82]

474.   On information and belief, Apple, starting in 2012 had worked with major corporations to deploy FairPlay Streaming in applications and on Apple TV.[83]

475.   Apple's documentation states that FairPlay Streaming "securely delivers keys to Apple mobile devices, Apple TV, and Safari on OS X, which will enable playback of encrypted video content."[84]

476.   Apple makes, sells, offers to sell, imports, and/or uses the Apple iTunes Store ("iTunes"). FairPlay Streaming is built into iTunes.[85]

477.   Apple makes, sells, offers to sell, imports, and/or uses iOS 6.0 and above ("iOS"). FairPlay Streaming is built into iOS 6.0 and above. [86]

478.   Apple makes, sells, offers to sell, imports, and/or uses Apple TV ("Apple TV"). FairPlay Streaming is built into Apple TV.[87]

479.   Apple makes, sells, offers to sell, imports, and/or uses the Apple Safari browser for iOS and OS X ("Safari"). FairPlay Streaming is built into Safari.[88]

---

[82] *Roger Pantos, Content Protection for HTTP Live Streaming* at 1-20, APPLE WORLD WIDE DEVELOPER CONFERENCE SESSION 502 (2015).

[83] *Roger Pantos, Transcription of Content Protection for HTTP Live Streaming*, APPLE WORLD WIDE DEVELOPER CONFERENCE SESSION 502 (2015) ("We have been working for the past three years with some of our major content partners to help them deploy FairPlay Streaming in their apps and on Apple TV.").

[84] *FairPlay Streaming Programming Guide: About FairPlay Streaming* at 6, APPLE TVOS DEVELOPER LIBRARY (2015).

[85] iTunes is an application included in iOS. *See* iOS Security Guide 7-8 (June 2015), https://www.apple.com/business/docs/iOS_Security_Guide.pdf.

[86] *Roger Pantos, Content Protection for HTTP Live Streaming* at 7, APPLE WORLD WIDE DEVELOPER CONFERENCE SESSION 502 (2015).

[87] *Id.*

480.   Apple makes, sells, offers to sell, imports, and/or uses OS X 10.10.4 or later versions ("OS X"). FairPlay Streaming is built into OS X.[89]

481.   Apple builds and offers to its customers the applications, services, and devices that incorporate Apple FairPlay Streaming. Products and services that have FairPlay Streaming built in include iTunes, iOS, Apple TV, Safari, and OS X (collectively, the "Apple '368 Products").

482.   Apple's documentation describes FairPlay Streaming as built into iOS, Apple TV and OS X.

483.   On information and belief, the Apple '368 Products are available to businesses and individuals throughout the United States.

484.   On information and belief, the Apple '368 Products are provided to businesses and individuals located in the Eastern District of Texas.
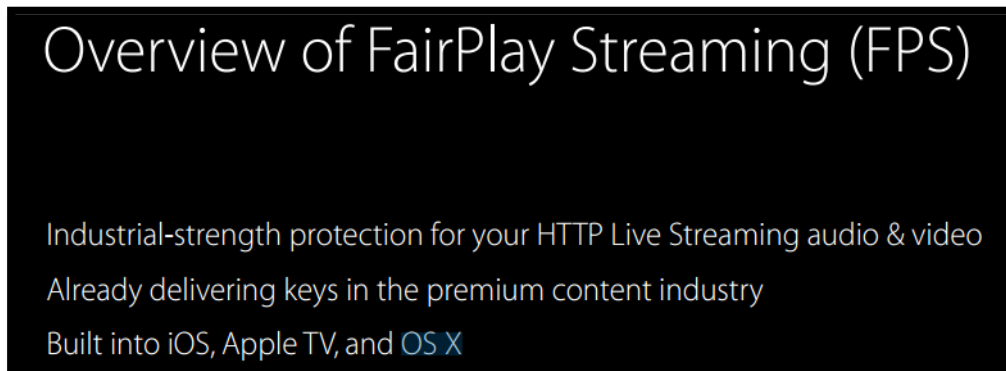
Roger Pantos, Content Protection for HTTP Live Streaming at 8, APPLE WORLD WIDE DEVELOPER CONFERENCE SESSION 502 (2015).

485.   Apple executives have stated "FairPlay [Streaming] provides great security and great battery life."[90]

---

[88] *Id.* at 82-88.

[89] *Id.* at 6, 8, 65-88.

[90] *Roger Pantos, Transcription of Content Protection for HTTP Live Streaming*, APPLE WORLD WIDE DEVELOPER CONFERENCE SESSION 502 (2015)

486.   Apple FairPlay Streaming has been incorporated into solutions available from companies throughout the United States, including: Irdeto,[91] Arris,[92] and Bright Cove.[93]

487.   On information and belief, Apple FairPlay Streaming stores a plurality of digital records (e.g., iTunes Store digital movie and TV show assets) and respective access rules for each digital record (e.g., asset-specific rules regarding the who, what, when, where, and how of allowed access) in a computer memory associated with a server system (e.g., the Apple iTunes Store server system).

488.   On information and belief, the iTunes Server system receives (e.g., via an http GET request to http://ax.phobos.apple.com.edgesuite.net/WebObjects/MZSearch.woa/wa/se) a request for access from a remote computer (e.g., a remote iOS mobile device, Mac computer, or AppleTV), to access a digital record stored in the computer memory (e.g., an iTunes Store movie or TV show asset stored in the iTunes Store server system).
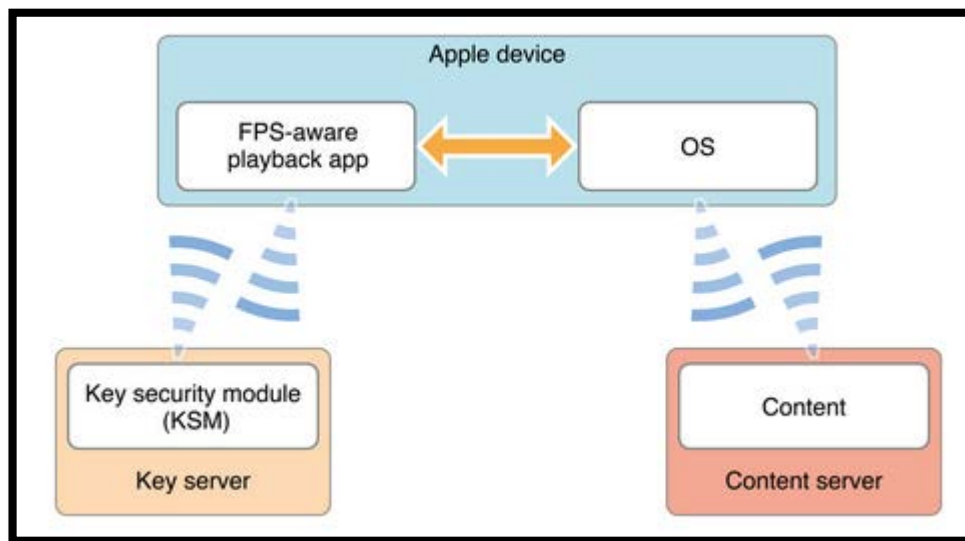
489.   On information and belief, Apple FairPlay Streaming validates, by the server system, the received request to access the digital record by applying a respective set of access rules for the digital record stored in the computer memory.

490.   The below diagram from Apple's FairPlay Streaming documentation shows the key and content exchange for Apple FairPlay Streaming.

---

[91] Irdeto is headquartered in Netherlands with offices in Eagan Minnesota. *Irdeto FairPlay Streaming Solution*, IRDETO WEBSITE, http://irdeto.com/partners/fairplay-compliant-apple-streaming.html.

[92] Arris is headquartered in Suwanee, Georgia. A*rris FairPlay Streaming Solution*, ARRIS WEBSITE, http://www.arris.com/products/fairplay-streaming/.

[93] Brightcove is headquartered in Australia with its United States headquarters in Boston, Massachusetts. F*airPlay Streaming + Brightcove Once,* BRIGHTCOVE WEBSITE, http://go.brightcove.com/bc-apple-fps/ ("The latest version also supports FairPlay Streaming, Apple's digital rights management (DRM) technology").
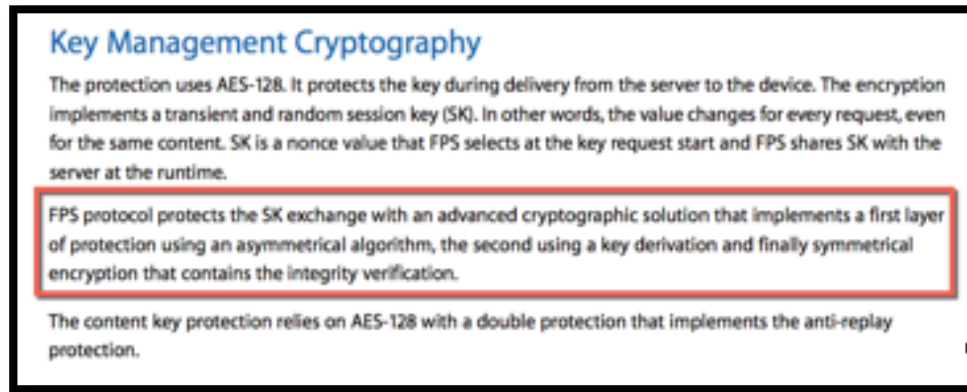
Apple FairPlay Streaming Overview at 4, APPLE DEVELOPER DOCUMENTATION (2015).

491.   On information and belief, the Apple '368 Products retrieve, by the server system, a public key having an associated private key, and associating a logging wrapper having a respective session key with the digital record, after validating the received request, wherein the session key is distinct from the public key and the private key.

492.   On information and belief, the iTunes Store server system retrieves a public key having an associated private key in order to implement a first layer of cryptographic protection using an asymmetrical algorithm. As a particular example, the iTunes Store server system retrieves, e.g., a client-specific RSA public key (having an associated client-specific RSA private key) from a digital certificate associated with the content request.

493.   The below documentation from Apple's FairPlay Streaming documentation states that the FairPlay Streaming protocol implements a first layer of protection using an asymmetric algorithm.
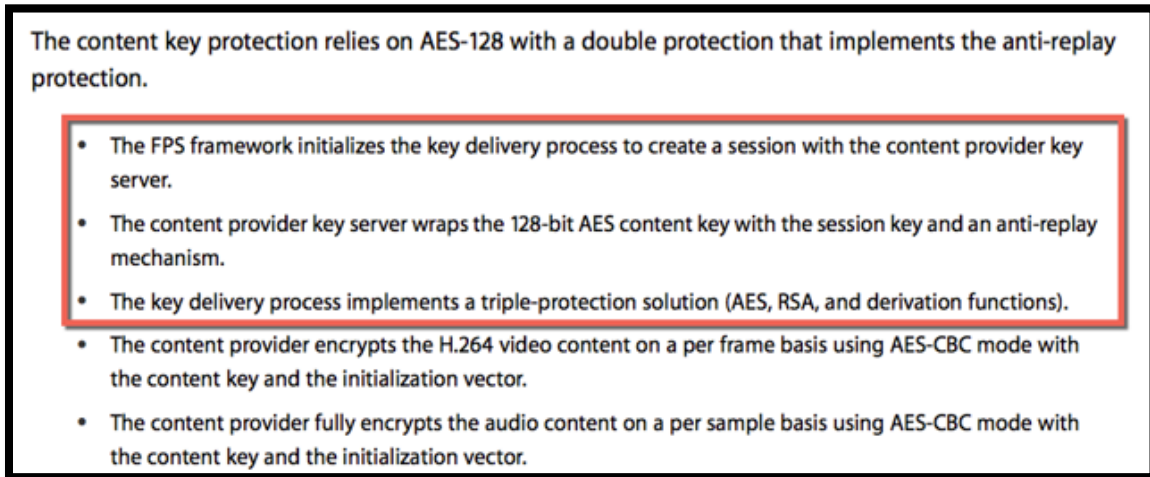
Key Management Cryptography

The protection uses AES-128. It protects the key during delivery from the server to the device. The encryption implements a transient and random session key (SK). In other words, the value changes for every request, even for the same content. SK is a nonce value that FPS selects at the key request start and FPS shares SK with the server at the runtime.

FPS protocol protects the SK exchange with an advanced cryptographic solution that implements a first layer of protection using an asymmetrical algorithm, the second using a key derivation and finally symmetrical encryption that contains the integrity verification.

The content key protection relies on AES-128 with a double protection that implements the anti-replay protection.

Apple FairPlay Streaming Overview at 4, APPLE DEVELOPER DOCUMENTATION (2015).

494.   On information and belief, the Apple FairPlay Streaming system registers a FairPlay Streaming application with an X.509 Certificate Signing request linked to a private key associated with the requesting device. The requesting device receives an Apple FairPlay Streaming Certificate encoded with the X.509 standard distinguished encoding rules.

495.   On information and belief, after validating a received request, the iTunes Store server system associates a logging wrapper having a respective session key with the digital record. For example, the iTunes Store server associates a secure lease logging wrapper having a respective session key with the digital record.

496.   On information and belief, the Apple FairPlay Streaming session key is distinct from the public key and the private key (e.g., the client-specific RSA public and private keys).

497.   The below documentation from Apple shows that FairPlay Streaming protects the session key exchange with an advanced cryptographic solution that implements a first layer of protection using an asymmetric algorithm, the second using a key derivation and finally symmetrical encryption that contains the integrity verification.

The content key protection relies on AES-128 with a double protection that implements the anti-replay protection.

- The FPS framework initializes the key delivery process to create a session with the content provider key server.
- The content provider key server wraps the 128-bit AES content key with the session key and an anti-replay mechanism.
- The key delivery process implements a triple-protection solution (AES, RSA, and derivation functions).
- The content provider encrypts the H.264 video content on a per frame basis using AES-CBC mode with the content key and the initialization vector.
- The content provider fully encrypts the audio content on a per sample basis using AES-CBC mode with the content key and the initialization vector.

Apple FairPlay Streaming Overview at 5, APPLE DEVELOPER DOCUMENTATION (2015)

498.   On information and belief, the Apple '368 Products encrypt and send, by the server system, the requested digital record, which has been validated, using the public key and the session key to encrypt the digital record.

499.   On information and belief, one or more of the Apple '368 Products include encryption technology.

500.   On information and belief, one or more of the Apple '368 Products enable sending encrypted information through an intermediary where the intermediary is not able to view the unencrypted message.

501.   On information and belief, the iTunes Store server system encrypts and sends the requested digital record (e.g., iTunes Store movie or television show) which has been validated, using the public key (e.g., the client-specific RSA public key) and the session-specific content key to encrypt the digital record.

502.   The below documentation from Apple shows that FairPlay Streaming protects the key during delivery from the server to the device. The encryption implements a transient and random session key.

138

Roger Pantos, *Content Protection for HTTP Live Streaming* at 39, APPLE WORLD WIDE
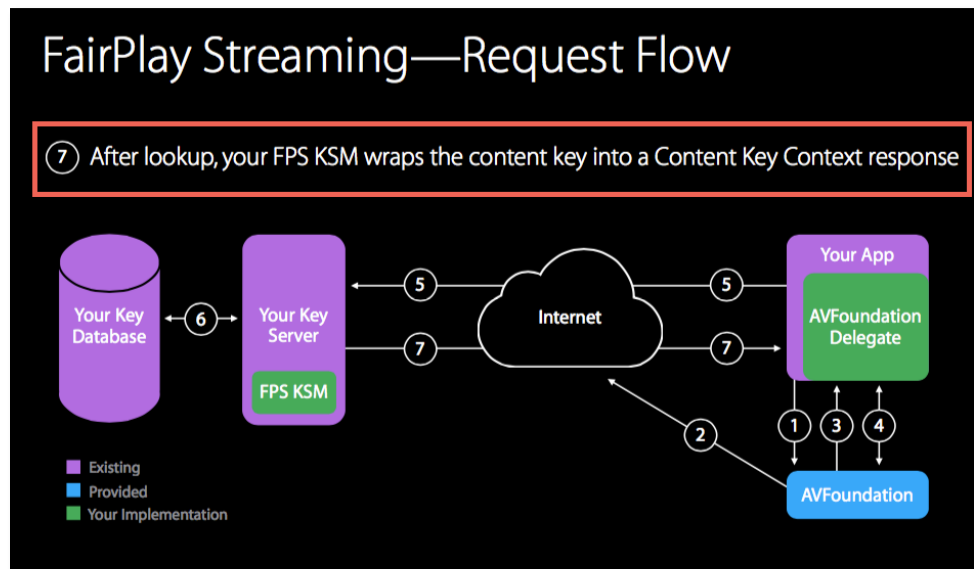
DEVELOPER CONFERENCE SESSION 502 (2015).

503.   On information and belief, the Apple '368 Products receive and decrypt the encrypted record, by the remote computer, using the private key, and the session key in conjunction with the logging wrapper.

504.   On information and belief, the Apple '368 Products receive a set of access rules associated with information made available through the Apple '368 Products system.

505.   The below image from the iTunes Package Music Specification 5.0.1 shows the access rules that are associated with information made available on the Apple '368 Products' system.

```
</checksum>
                    </data_file>
                </asset>
            </assets>
            <products>
                <product>
                    <territory>US</territory>
                    <cleared_for_sale>true</cleared_for_sale>
                    <cleared_for_hd_sale>true</cleared_for_hd_sale>
                    <wholesale_price_tier>3</wholesale_price_tier>
                    <hd_wholesale_price_tier>1</hd_wholesale_price_tier>
                    <preorder_sales_start_date>2011-02-10</preorder_sales_start_date>
                    <sales_start_date>2011-03-12</sales_start_date>
                    <cleared_for_vod>true</cleared_for_vod>
                    <vod_type>New Release</vod_type>
                    <available_for_vod_date>2012-11-12</available_for_vod_date>
                    <unavailable_for_vod_date>2013B-11-12</unavailable_for_vod_date>
                    <physical_release_date>2007-08-01</physical_release_date>
                    <cleared_for_hd_vod>false</cleared_for_hd_vod>
                </product>
            </products>
        </video>
    </package>
```

iTunes Package Music Specification 5.0.1 at 17, APPLE ITUNES MUSIC SPECIFICATION (showing access rules including "Wholesale_Price Tier").

506.   On information and belief, the Apple '368 Products use specially designed, tamper resistant Apple-only (i.e., not open to third party developers or end users) system hardware and software on the remote computer (e.g., iOS mobile device; Mac computer; Apple TV). The Apple '368 Products contain functionality to receive and decrypt the encrypted iTunes Store digital media asset using the private key (e.g., the client-specific RSA private key) and the session key (e.g., the session-specific content key) in conjunction with the logging wrapper (e.g., the secure lease logging wrapper).

507.   The below documentation from Apple establishes that FairPlay Streaming send content keys to a player device using tamper resistant techniques.

- FPS supports the H.264 video codec and AAC-LC, HE-AACV1-2, and AC-3 audio codecs. Audio codecs may vary for Safari's FPS.
- The key handling and the content decryption occur on the kernel of the iOS device. In other words, the content as well as the content key are kept on the device kernel for the decryption.
- FPS always enforces HDCP for each protected content block.
- FPS does not support persistence of the security material.

Apple FairPlay Streaming Overview at 4, APPLE DEVELOPER DOCUMENTATION (2015).

508.   On information and belief, only specially designed, tamper resistant Apple-368

Products can be used to receive and decrypt an encrypted iTunes Store media asset—both as a

technological matter and as a contractual requirement Apple imposes on developers.

509.   The below presentation from Apple's 2015 Worldwide Developers Conference

evidences that FairPlay Streaming is responsible for relaying the key requests from AV

foundation to a backend and returning the response from the backend back to AV foundation.
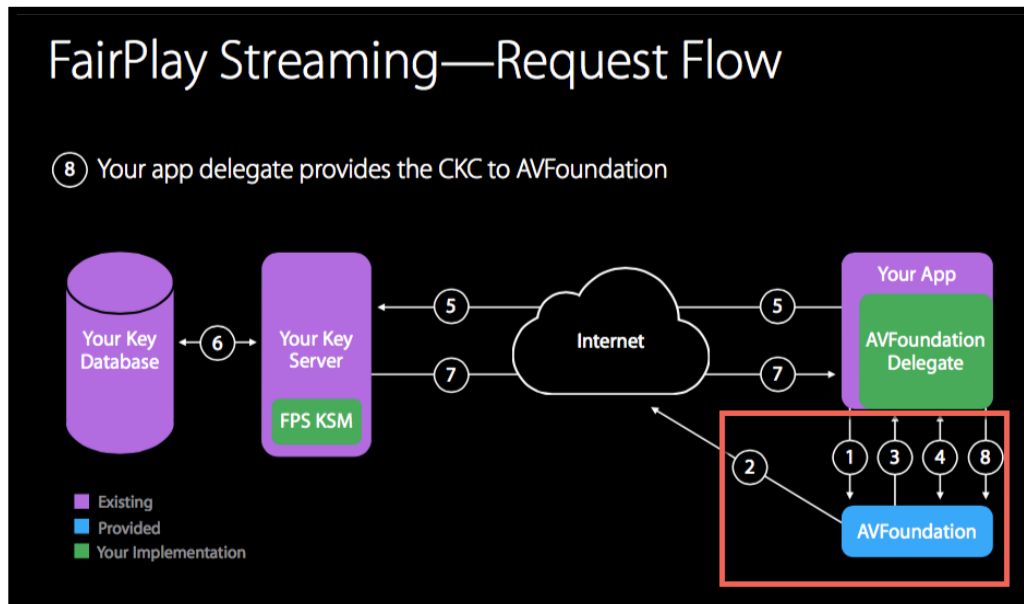
Roger Pantos, *Content Protection for HTTP Live Streaming* at 40, APPLE WORLD WIDE
DEVELOPER CONFERENCE SESSION 502 (2015).

510.   On information and belief, Apple FairPlay Streaming generates by the logging

wrapper (e.g., the secure lease logging wrapper), at the remote computer (e.g., the iOS mobile

device; Mac computer; or AppleTV) an SPV logging event (e.g., a halted playback message or a

lease renewal request).

511.   On information and belief, the Apple '368 Products record a logging event in an

access log.

512.   On information and belief, the iTunes Store server system records the logging

event (e.g., the client's halted playback message or lease renewal request) in an access log—e.g.,

an account-specific access log used to track simultaneous playback information for a user

account and/or a content partner-specific access log used to track granular content usage information for auditing, compensation, and/or analytics purposes.

513.   The below documentation from Apple's FairPlay Streaming documentation shows some of the fields that are recorded as a logging event in an access log.

Table 5-1   Media playback state TLLV

Field name	Byte range	Description
TLLV tag	0-7	An 8-byte value of 0xeb8efdf2b25ab3a0.
Total Length	8-11	The total length of this TLLV block in bytes. The total length is determined by the amount of padding at the end of the block, if any; it must be a multiple of 16 and greater than 32.
Value Length	12-15	The length of the content of this TLLV block in bytes, 0x00000010 (decimal 16).
Creation Date	16-19	The time in seconds from Jan 1, 1970 to the time when the SPC was created.
Playback State	20-23	The playback state of the Apple device at the time the SPC was created. Possible values are listed in Table 5-2 (page 36).
Session ID	24-31	An ID that represents the playback of a media content independently of its bit rates and content keys.
Padding	32-n (padding_size)	Random values to fill out the TLLV to a multiple of 16 bytes. See the description of the Padding field in Table 2-2 (page 14).

FairPlay Streaming Programming Guide at 36, APPLE DEVELOPER DOCUMENTATION (2015)

514.   On information and belief, the Apple '368 Products encrypt one or more records using an encryption scheme with a rolling code.

515.   On information and belief, Apple requires third parties to enter into a restrictive covenant for access to information. The below excerpt from Apple's Terms & Conditions is indicative of one exemplar of a "restrictive covenant" that Apple requires of third parties.
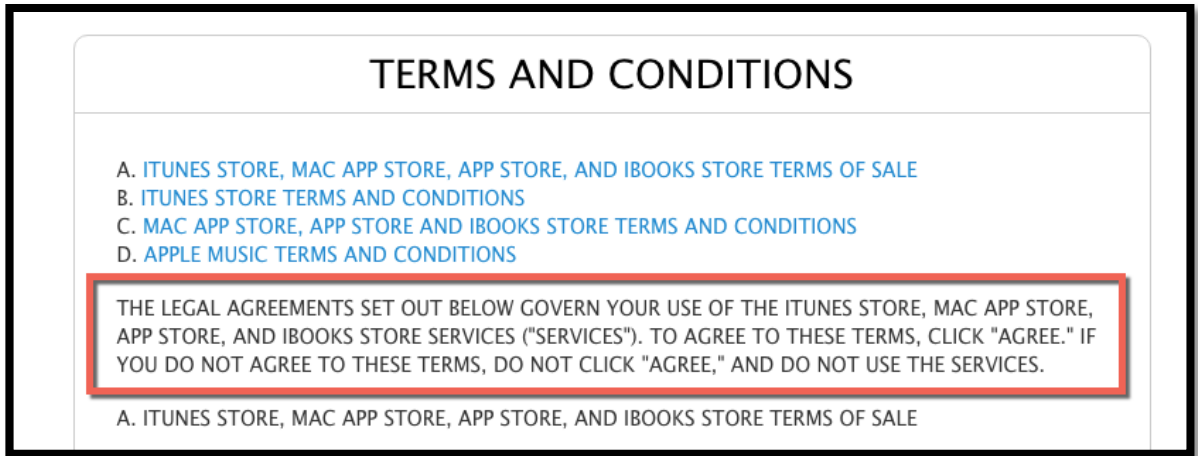
iTunes Store Terms and Conditions, APPLE WEBSITE (2015),
http://www.apple.com/legal/internet-services/itunes/us/terms.html

516.   On information and belief, Apple has directly infringed and continues to directly

infringe the '368 patent by, among other things, making, using, offering for sale, and/or selling

products and/or services for secure three-party communications, including but not limited to, the

Apple '368 Products, which include infringing encryption technologies. Such products and/or

services include, by way of example and without limitation, Apple FairPlay Streaming content

protection, Apple iTunes Store, Apple iTunes client software, Apple Safari browser (for iOS and

OS X), Apple iOS mobile devices (e.g., iPhone, iPad, iPod Touch) and system software, Mac OS

X computers and system software, AppleTV devices and system software, iMessage, Apple

FaceTime, Apple Handoff, and Apple iOS mobile devices (e.g., iPhone, iPad, iPod Touch).

517.   By making, using, testing, offering for sale, and/or selling encryption products

and services, including but not limited to the Apple '368 Products, Apple has injured St. Luke

and is liable to St. Luke for directly infringing one or more claims of the '368 patent, including at

least claims 1-3, 7-8, 18, 21-22, 24, 29-31, 35, 59, 73, 74, and 133, pursuant to 35 U.S.C.

§ 271(a).

518.   On information and belief, Apple also infringes indirectly the '368 patent by

active inducement under 35 U.S.C. § 271(b).

143

519.   Apple has had knowledge of the '368 patent since at least service of this Complaint or shortly thereafter, and on information and belief, Apple knew of the '368 patent and knew of its infringement, including by way of this lawsuit.

520.   On information and belief, Apple intended to induce patent infringement by third-party customers and users of the Apple '368 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Apple specifically intended and was aware that the normal and customary use of the accused products would infringe the '368 patent. Apple performed the acts that constitute induced infringement, and would induce actual infringement, with the knowledge of the '368 patent and with the knowledge, that the induced acts would constitute infringement. For example, Apple provides the Apple '368 Products that have the capability of operating in a manner that infringe one or more of the claims of the '368 patent, including at least claims 1-3, 7-8, 18, 21-22, 24, 29-31, 35, 59, 73-74, and 133, and Apple further provides documentation and training materials that cause customers and end users of the Apple '368 Products to utilize the products in a manner that directly infringe one or more claims of the '368 patent. By providing instruction and training to customers and end-users on how to use the Apple '368 Products in a manner that directly infringes one or more claims of the '368 patent, including at least claims 1-3, 7-8, 18, 21-22, 24, 29-31, 35, 59, 73-74, and 133, Apple specifically intended to induce infringement of the '368 patent. On information and belief, Apple engaged in such inducement to promote the sales of the Apple '368 Products, *e.g.,* through Apple's user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '368 patent.[94] Accordingly, Apple has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '368 patent, knowing that such use constitutes infringement of the '368 patent.

---

[94] *See e.g.*, iOS Security Guide (June 2015); FairPlay Streaming Overview (July 8, 2015); WWDC15 Session 502 – Content Protection for HTTP Live Streaming Presentation; iTunes Package Film Specification 5.0 (May 22, 2012).

521.   To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '368 patent.

522.   As a result of Apple's infringement of the '368 patent, St. Luke has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Apple's infringement, but in no event less than a reasonable royalty for the use made of the invention by Apple together with interest and costs as fixed by the Court.

<div align="center"><u>COUNT VII</u>
<u>INFRINGEMENT OF U.S. PATENT NO. 8,498,941</u></div>

523.   St. Luke references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

524.   Apple makes, sells, offers to sell, imports, and/or uses products called the Apple iTunes Store, Apple iTunes client software for iOS, OS X, and Windows (collectively, "iTunes").

525.   Apple makes, sells, offers to sell, imports, and/or uses Apple iOS mobile devices (e.g., iPhone, iPad, iPod Touch) and system software (collectively, "iOS").

526.   Apple makes, sells, offers to sell, imports, and/or uses products and services that contain Apple infringing functionality, including iTunes and iOS (collectively, "Apple '941 Products").

527.   On information and belief, the iTunes Store server searches the plurality of automated electronic databases (e.g., the respective iTunes Store Movie, iTunes Store TV Show, iTunes Store Music, App Store, iBooks Store, iTunes Store Audiobook, iTunes Store Music Video, iTunes Store Podcast, and iTunes U automated electronic databases) to find records relating to an entity corresponding to the request (e.g., electronic music songs, albums, and music videos performed by the Hip-Hop/Rap artist Mac Miller), and records having connections to records corresponding to the request, relating to transactions, relationships or communications between the entity and another entity (e.g., fan-generated iPhone and iPad apps devoted to Mac Miller; music podcasts with one or more recent episodes discussing and/or interviewing Mac

Miller; TV episodes and seasons on which Mac Miller was a guest star and/or musical guest; etc.).

528.   On information and belief, the iTunes Store server, by at least one automated processor, applies a set of access rules associated with each found record—for example, a set of iTunes Connect metadata rules specifying variations in pricing, media quality, in-content advertising, and/or overall availability of each found record (e.g., each found digital music, movie, TV show, app, eBook, audiobook, music video, podcast, or coursework record) based one or more requestor attributes (e.g., geographic location, date and/or time, client hardware and/or software platform, age, and purchase history)—to produce a set of accessible records, at a server device.

529.   On information and belief, the Apple '941 Products perform methods for controlling access to a plurality of records provided within a plurality of automated electronic databases, each record having an associated set of access rules.

530.   The below documentation from Apple shows the Metadata that can be associated with information on the iTunes server.

iTunes Extras Package Specification 5.2 Revision 1 at 55, APPLE ITUNES DOCUMENTATION (2014).

531.   On information and belief, the iTunes Store server logs, by at least one automated processor, at least the request for access—e.g., as part of Apple's comprehensive usage audit and analytics framework for developers and content providers.

532.   The below screen capture from Apple's website shows that data is stored by Apple as part of a comprehensive usage audit that is accessible by content developers.

Metrics and Measures

Term	Definition	Metric Type
Active Devices	The number of devices with at least one session during the selected period. Only devices with iOS 8 or later are included. Totals are based on app users who agree to share their data with you.	Usage
Active in Last 30 Days	The number of active devices with at least one session during the previous 30 days. Totals are based on app users who agree to share their data with you.	Usage
App Store Views	The number of times your app's App Store page has been viewed on a device using iOS 8 or later. Although apps can be downloaded without visiting the app's App Store product page, such as directly from search results, only App Store product page views are counted.	Sales
App Units	The number of first-time app purchases made on the App Store using iOS 8 or later. App updates, downloads from the same Apple ID onto other devices, and redownloads to the same device are not counted. Family Sharing downloads are included for free apps, but not for paid apps.	Sales
In-App Purchases	The number of first-time purchases of an In-App Purchase on a device using iOS 8 or later. Restored In-App Purchases, whether on the same or on a different device, are not counted.	Sales
Installations	The total number of times your app has been installed on an iOS device with iOS 8 or later. Redownloads on the same device, downloads to multiple devices sharing the same Apple ID, and Family Sharing installations are included. App updates aren't counted. Totals are based on app users who agree to share their data with you.	Usage
Sales	The total amount billed to customers for purchasing apps, app bundles, and In-App Purchases. Taxes are only included in the sales if those taxes were included in the App Store price. Note that sales totals are not the same as your proceeds. You can see your payments in Payments and Financial Reports on iTunes Connect if you have the Admin or Finance roles.	Sales
Sessions	The number of times the app has been used for at least two seconds. If the app is in the background and is later used again, that counts as another session. Totals are based on app users who agree to share their data with you.	Usage

iTunes Connect App Analytics Guide v.1 at 13, APPLE ITUNES DOCUMENTATION (2015).

533.   On information and belief, the iTunes Store server communicates the set of accessible electronic media records to the iTunes Store client for display to the requestor (e.g., via an XML Store Bag data structure).

147

534.   On information and belief, the Apple '941 Products include the functionality for an access rule associated with a respective record is defined by the entity to which the record relates where the entity is a content provider—e.g., an independent and/or self-publishing musician, author, podcast host, or developer.

535.   On information and belief, Apple has directly infringed and continues to directly infringe the '941 patent by, among other things, making, using, offering for sale, and/or selling products and/or services for secure three-party communications, including but not limited to, the Apple '941 Products, which include infringing encryption technologies. Such products and/or services include, by way of example and without limitation, Apple iTunes Store, Apple iTunes client software for iOS, OS X, and Windows, Apple iOS mobile devices (e.g., iPhone, iPad, iPod Touch) and system software, and Mac OS X computers and system software.

536.   By making, using, testing, offering for sale, and/or selling encryption products and services, including but not limited to the Apple '941 Products, Apple has injured St. Luke and is liable to St. Luke for directly infringing one or more claims of the '941 patent, including at least claims 16 and 18-19, pursuant to 35 U.S.C. § 271(a).

537.   On information and belief, Apple also infringes indirectly the '941 patent by active inducement under 35 U.S.C. § 271(b).

538.   Apple has had knowledge of the '941 patent since at least service of this Complaint or shortly thereafter, and on information and belief, Apple knew of the '941 patent and knew of its infringement, including by way of this lawsuit.

539.   On information and belief, Apple intended to induce patent infringement by third-party customers and users of the Apple '941 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Apple specifically intended and was aware that the normal and customary use of the accused products would infringe the '941 patent. Apple performed the acts that constitute induced infringement, and would induce actual infringement, with the knowledge of the '941 patent and with the knowledge, that the induced acts would constitute infringement. For

148

example, Apple provides the Apple '941 Products that have the capability of operating in a manner that infringe one or more of the claims of the '941 patent, including at least claims 16 and 18-19, and Apple further provides documentation and training materials that cause customers and end users of the Apple '941 Products to utilize the products in a manner that directly infringe one or more claims of the '941 patent. By providing instruction and training to customers and end-users on how to use the Apple '941 Products in a manner that directly infringes one or more claims of the '941 patent, including at least claims 16 and 18-19, Apple specifically intended to induce infringement of the '941 patent. On information and belief, Apple engaged in such inducement to promote the sales of the Apple '941 Products, *e.g.,* through Apple's user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '941 patent.[95] Accordingly, Apple has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '941 patent, knowing that such use constitutes infringement of the '941 patent.

540.   To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '941 patent.

541.   As a result of Apple's infringement of the '941 patent, St. Luke has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Apple's infringement, but in no event less than a reasonable royalty for the use made of the invention by Apple together with interest and costs as fixed by the Court.

---

[95] *See e.g.*, iTunes 12.2.25 client software for Mac (OS X Yosemite 10.10.5 on Mac Pro (Late 2013)); iTunes Store app for iPhone (iOS 8.4.1 on iPhone 6); iTunes Store app for iPad (iOS 8.4.1 on iPad 3); iTunes Package Film Specification 5.0 (May 22, 2012); iTunes Package Music Specification 5.2 (Apr. 10, 2014); iTunes Extras Package Specification 5.2 Rev. 1 (Aug. 12, 2014); iBooks Asset Guide 5.1 Rev 2 (Aug. 13, 2013); iBooks Publisher User Guide 10 (Mar. 11, 2015); iTunes Connect Programming Guide (Apr. 30, 2015).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff St. Luke respectfully requests that this Court enter:

A.   A judgment in favor of Plaintiff St. Luke that Apple has infringed, either literally and/or under the doctrine of equivalents, the '237 patent, the '017 patent, the '591 patent, the '181 patent, the '247 patent, the '368 patent, and/or the '941 patent.

B.   An award of damages resulting from Apple's acts of infringement in accordance with 35 U.S.C. § 284;

C.   A judgment and order requiring Apple to provide accountings and to pay supplemental damages to St. Luke, including, without limitation, prejudgment and post-judgment interest; and

D.   Any and all other relief to which St. Luke may show itself to be entitled.

JURY TRIAL DEMANDED

Pursuant to Rule 38 of the Federal Rules of Civil Procedure, St. Luke requests a trial by jury of any issues so triable by right.

Dated: September 24, 2015

Respectfully submitted,

/s/ Elizabeth L. DeRieux   _____
Elizabeth L. DeRieux (TX Bar No. 05770585)
D. Jeffrey Rambin (TX Bar No. 00791478)
CAPSHAW DERIEUX, LLP
114 E. Commerce Ave.
Gladewater, Texas 75647
Telephone: 903-236-9800
Facsimile: 903-236-8787
E-mail: ederieux@capshawlaw.com
E-mail: jrambin@capshawlaw.com

OF COUNSEL:

Matt Olavi (CA SB No. 265945)
Brian J. Dunne (CA SB No. 275689)
OLAVI & DUNNE LLP
816 Congress Ave., Ste. 1620
Austin, Texas 78701
Telephone: 512-717-4485
Facsimile: 512-717-4495
E-mail: molavi@olavidunne.com
E-mail: bdunne@olavidunne.com

Dorian S. Berger (CA SB No. 264424)
Daniel P. Hipskind (CA SB No. 266763)
OLAVI & DUNNE LLP
1880 Century Park East, Ste. 815
Los Angeles, CA 90067
Telephone: 213-516-7900
Facsimile: 213-516-7910
E-mail: dberger@olavidunne.com
E-mail: dhipskind@olavidunne.com

Attorneys for St. Luke Technologies, LLC

151